Códigos electrónicos

Código de Administración Electrónica

Selección y ordenación:
Secretaría General de Administración Digital

Edición actualizada a 21 de julio de 2023

MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

BOLETÍN OFICIAL DEL ESTADO

La última versión de este Código en PDF y ePUB está disponible para su descarga **gratuita** en:
www.boe.es/biblioteca_juridica/

Alertas de actualización en Mi BOE: www.boe.es/mi_boe/

Para adquirir el Código en formato papel: tienda.boe.es

NIPO (PDF): (BOE) 007-15-010-7
NIPO (PDF): (MINHAP) 630-15-048-6
NIPO (Papel): (BOE) 007-15-008-9
NIPO (Papel): (MINHAP) 630-15-046-5
NIPO (ePUB): (BOE) 007-15-009-4
NIPO (ePUB): (MINHAP) 630-15-047-0
ISBN: 978-84-340-2162-4
Depósito Legal: M-4635-2015

Catálogo de Publicaciones de la Administración General del Estado
cpage.mpr.gob.es

Agencia Estatal Boletín Oficial del Estado
Avenida de Manoteras, 54
28050 MADRID
www.boe.es

SUMARIO

INSTRUCCIONES TÉCNICAS DE SEGURIDAD

SISTEMA DE VERIFICACIÓN DE DATOS

CONTRATACIÓN ADMINISTRATIVA Y EMPLEO DE MEDIOS ELECTRÓNICOS

FACTURA ELECTRÓNICA

SEGURIDAD SOCIAL

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

REUTILIZACIÓN DE LA INFORMACIÓN DEL SECTOR PÚBLICO

COMUNICACIÓN DIGITAL

BOLETÍN OFICIAL DEL ESTADO

ACCESIBILIDAD

PROTECCIÓN DE DATOS

ADMINISTRACIÓN JUDICIAL ELECTRÓNICA

ÍNDICE SISTEMÁTICO

IDENTIFICACIÓN, FIRMA ELECTRÓNICA Y REPRESENTACIÓN

REGISTROS ELECTRÓNICOS

NOTIFICACIÓN ELECTRÓNICA

ARCHIVO ELECTRÓNICO DE DOCUMENTOS

NORMAS TÉCNICAS DE INTEROPERABILIDAD

INSTRUCCIONES TÉCNICAS DE SEGURIDAD

SISTEMA DE VERIFICACIÓN DE DATOS

CONTRATACIÓN ADMINISTRATIVA Y EMPLEO DE MEDIOS ELECTRÓNICOS

FACTURA ELECTRÓNICA

SEGURIDAD SOCIAL

TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA

REUTILIZACIÓN DE LA INFORMACIÓN DEL SECTOR PÚBLICO

COMUNICACIÓN DIGITAL

BOLETÍN OFICIAL DEL ESTADO

ACCESIBILIDAD

PROTECCIÓN DE DATOS

ADMINISTRACIÓN JUDICIAL ELECTRÓNICA

§ 1

Nota del autor

Última modificación: 16 de diciembre de 2019

La transformación digital de la Administración, que da lugar a la denominada administración electrónica, o según el lenguaje más reciente, a la administración digital, es ineludible y se caracteriza por su alcance global, de forma que su plena realización requiere de varios pilares que se relacionan y evolucionan de una forma dinámica a lo largo del tiempo; a saber, una estrategia continuada de medio plazo; el marco legal que aporta la seguridad jurídica; la cooperación y la gobernanza, imprescindibles en un escenario con múltiples actores interconectados que han de colaborar para facilitar la prestación de los servicios; y las propias infraestructuras tecnológicas y los servicios que aportan la realidad práctica. La transformación digital permite hacer una administración más eficiente, centrada en las necesidades de ciudadanos y empresas, más abierta, participativa y transparente. No es un mero proceso tecnológico, sino que requiere una visión multidisciplinar que, afecta a los procesos, que han de simplificarse para aprovechar las oportunidades de la sociedad digital, a los diversos actores implicados (funcionarios, ciudadanos y empresas) que han de adquirir una nueva perspectiva y dotarse de competencias digitales, a la tecnología que ofrece oportunidades pero que también suscita riesgos, a la gestión de los datos en un escenario crecientemente datacéntrico, y finalmente a la (ciber)seguridad imprescindible para la protección de la información manejada y los servicios prestados.

En este contexto complejo, el marco legal es un poderoso resorte para movilizar la Administración en pos de esta transformación digital; cabe afirmar que el mismo constituye hoy en día un activo, una oportunidad que se ha de aprovechar, sin perjuicio de que sea necesario su constante perfeccionamiento y evolución. El marco legal constituye, por tanto, una formidable palanca de acción no exenta de retos y dificultades para su plena aplicación.

España cuenta, como fruto de un esfuerzo colectivo, multidisciplinar y continuado a lo largo del tiempo, con un marco legal, en evolución casi de forma continuada, que trata, de forma exhaustiva, todos aquellos aspectos necesarios para la implantación de la administración digital, desarrollada bajo el principio de seguridad jurídica, adecuado todo ello a la realidad que impone la transformación digital, que proporciona unas reglas de juego que facilitan la extensión a gran escala de la prestación y uso de los servicios públicos digitales. Este marco legal se ha constituido a partir de hitos tales como la Ley 11/2007, de 22 de junio, y sus desarrollos, y las leyes 39/2015 y 40/2015, ambas de 1 de octubre.

La Secretaría General de Administración Digital promueve el Código de Administración Electrónica, compendio de la legislación relativa a la administración electrónica, para ofrecer una herramienta de interés y utilidad para los profesionales, gestores y estudiosos de la materia.

El Código incluye la legislación básica del tema, junto con otras cuestiones relacionadas: Administración electrónica (procedimiento administrativo común, régimen jurídico, esquemas nacionales de seguridad e interoperabilidad, instrumentos de las TIC en la AGE), Identificación, firma electrónica y representación, Registros electrónicos, Notificación electrónica, Archivo electrónico de documentos, Normas técnicas de interoperabilidad,

Instrucciones Técnicas de seguridad, Sistema de verificación de datos, Contratación administrativa y empleo de medios electrónicos, Factura electrónica, Seguridad social, Transparencia y acceso a la información pública, Reutilización de la información del sector público, Comunicación digital, Boletín oficial del estado, Accesibilidad, Protección de datos, Administración Judicial Electrónica. Para profundizar en ciertas cuestiones puede ser necesario acudir a otros códigos, tales como el de Archivos y Patrimonio Documental, el de Protección de Datos de Carácter Personal, o el de la Ciberseguridad.

No podemos olvidar, por otra parte, que España es un país de administración fuertemente descentralizada, por lo que esta legislación básica ha de completarse, en determinados casos, con normativa específica de desarrollo que nuestro marco competencial atribuye a Comunidades Autónomas y Entidades Locales. Finalmente, nos encontramos en un contexto europeo y el desarrollo de la agenda digital y del mercado único digital en Europa requiere del conocimiento y cumplimiento de la normativa comunitaria en la materia para hacer de Europa una sociedad cohesionada, que disminuya las cargas administrativas de las empresas en Europa, y aproveche las ventajas que proporciona la economía de escala de un mercado europeo.

La administración en papel ha dejado paso a la administración electrónica, en muchos casos ya de forma obligatoria para ciudadanos y empresas, incluso en la relación entre administraciones públicas. La automatización de procesos, la gestión de datos personales, la inclusión de técnicas de inteligencia artificial en los procedimientos administrativos y los riesgos de ciberseguridad del mundo de hoy crean un nuevo escenario con nuevos retos globales donde la ética, esencialmente unida a la normativa administrativa, jugará un papel protagonista en los próximos años para garantizar que la transformación digital contribuirá a reforzar el modelo de España y Europa en el mundo, con un desarrollo económico respetuoso, sostenible e inclusivo, que no deje a nadie atrás.

Fernando de Pablo Martín

Secretario General de Administración Digital

Miguel A. Amutio Gómez

Director de la División de Planificación y Coordinación de Ciberseguridad

NORMATIVA EUROPEA NO CONSOLIDADA

Reglamento (UE) nº910/2014 del Parlamento Europeo y del Consejo, de 23de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

https://www.boe.es/doue/2014/257/L00073-00114.pdf

http://data.europa.eu/eli/reg/2014/910/oj

Reglamento de Ejecución (UE) 2015/1501 de la Comisión, de 8 de septiembre de 2015, sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

https://www.boe.es/doue/2015/235/L00001-00006.pdf

http://data.europa.eu/eli/reg_impl/2015/1501/oj

Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) n° 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior

https://www.boe.es/doue/2015/235/L00037-00041.pdf

http://data.europa.eu/eli/dec_impl/2015/1506/oj

Reglamento (UE) nº 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.° 1024/2012

https://www.boe.es/doue/2018/295/L00001-00038.pdf

http://data.europa.eu/eli/reg/2018/1724/oj

Reglamento (UE) Nº 1025/2012, de 25 de octubre, del Parlamento Europeo y del Consejo, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión 1673/2006/CE del Parlamento Europeo y del Consejo

https://www.boe.es/doue/2012/316/L00012-00033.pdf

http://data.europa.eu/eli/reg/2012/1025/oj

Decisión de Ejecución (UE) 2017/863 de la Comisión, de 18 de mayo de 2017, por la que se actualiza la licencia EUPL de los programas informáticos de fuente abierta para seguir facilitando el intercambio y la reutilización de los programas desarrollados por las administraciones públicas Licencia Pública Europea EUPL (European Union Public Licence)

http://data.europa.eu/eli/dec_impl/2017/863/oj

§ 2

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 19 de octubre de 2022
Referencia: BOE-A-2015-10565

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

I

La esfera jurídica de derechos de los ciudadanos frente a la actuación de las Administraciones Públicas se encuentra protegida a través de una serie de instrumentos tanto de carácter reactivo, entre los que destaca el sistema de recursos administrativos o el control realizado por jueces y tribunales, como preventivo, a través del procedimiento administrativo, que es la expresión clara de que la Administración Pública actúa con sometimiento pleno a la Ley y al Derecho, como reza el artículo 103 de la Constitución.

El informe elaborado por la Comisión para la Reforma de las Administraciones Públicas en junio de 2013 parte del convencimiento de que una economía competitiva exige unas Administraciones Públicas eficientes, transparentes y ágiles.

En esta misma línea, el Programa nacional de reformas de España para 2014 recoge expresamente la aprobación de nuevas leyes administrativas como una de las medidas a impulsar para racionalizar la actuación de las instituciones y entidades del poder ejecutivo, mejorar la eficiencia en el uso de los recursos públicos y aumentar su productividad.

Los defectos que tradicionalmente se han venido atribuyendo a las Administraciones españolas obedecen a varias causas, pero el ordenamiento vigente no es ajeno a ellas, puesto que el marco normativo en el que se ha desenvuelto la actuación pública ha propiciado la aparición de duplicidades e ineficiencias, con procedimientos administrativos demasiado complejos que, en ocasiones, han generado problemas de inseguridad jurídica. Para superar estas deficiencias es necesaria una reforma integral y estructural que permita ordenar y clarificar cómo se organizan y relacionan las Administraciones tanto externamente, con los ciudadanos y empresas, como internamente con el resto de Administraciones e instituciones del Estado.

En coherencia con este contexto, se propone una reforma del ordenamiento jurídico público articulada en dos ejes fundamentales: las relaciones «ad extra» y «ad intra» de las

Administraciones Públicas. Para ello se impulsan simultáneamente dos nuevas leyes que constituirán los pilares sobre los que se asentará el Derecho administrativo español: la Ley del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley de Régimen Jurídico del Sector Público.

Esta Ley constituye el primero de estos dos ejes, al establecer una regulación completa y sistemática de las relaciones «ad extra» entre las Administraciones y los administrados, tanto en lo referente al ejercicio de la potestad de autotutela y en cuya virtud se dictan actos administrativos que inciden directamente en la esfera jurídica de los interesados, como en lo relativo al ejercicio de la potestad reglamentaria y la iniciativa legislativa. Queda así reunido en cuerpo legislativo único la regulación de las relaciones «ad extra» de las Administraciones con los ciudadanos como ley administrativa de referencia que se ha de complementar con todo lo previsto en la normativa presupuestaria respecto de las actuaciones de las Administraciones Públicas, destacando especialmente lo previsto en la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera; la Ley 47/2003, de 26 de noviembre, General Presupuestaria, y la Ley de Presupuestos Generales del Estado.

II

La Constitución recoge en su título IV, bajo la rúbrica «Del Gobierno y la Administración», los rasgos propios que diferencian al Gobierno de la Nación de la Administración, definiendo al primero como un órgano eminentemente político al que se reserva la función de gobernar, el ejercicio de la potestad reglamentaria y la dirección de la Administración y estableciendo la subordinación de ésta a la dirección de aquel.

En el mencionado título constitucional el artículo 103 establece los principios que deben regir la actuación de las Administraciones Públicas, entre los que destacan el de eficacia y el de legalidad, al imponer el sometimiento pleno de la actividad administrativa a la Ley y al Derecho. La materialización de estos principios se produce en el procedimiento, constituido por una serie de cauces formales que han de garantizar el adecuado equilibrio entre la eficacia de la actuación administrativa y la imprescindible salvaguarda de los derechos de los ciudadanos y las empresas, que deben ejercerse en condiciones básicas de igualdad en cualquier parte del territorio, con independencia de la Administración con la que se relacionen sus titulares.

Estas actuaciones «ad extra» de las Administraciones cuentan con mención expresa en el artículo 105 del texto constitucional, que establece que la Ley regulará la audiencia de los ciudadanos, directamente o a través de las organizaciones y asociaciones reconocidas por la Ley, en el procedimiento de elaboración de las disposiciones administrativas que les afecten, así como el procedimiento a través del cual deben producirse los actos administrativos, garantizando, cuando proceda, la audiencia a los interesados.

A ello cabe añadir que el artículo 149.1.18.ª de la Constitución Española atribuye al Estado, entre otros aspectos, la competencia para regular el procedimiento administrativo común, sin perjuicio de las especialidades derivadas de la organización propia de las Comunidades Autónomas, así como el sistema de responsabilidad de todas las Administraciones Públicas.

De acuerdo con el marco constitucional descrito, la presente Ley regula los derechos y garantías mínimas que corresponden a todos los ciudadanos respecto de la actividad administrativa, tanto en su vertiente del ejercicio de la potestad de autotutela, como de la potestad reglamentaria e iniciativa legislativa.

Por lo que se refiere al procedimiento administrativo, entendido como el conjunto ordenado de trámites y actuaciones formalmente realizadas, según el cauce legalmente previsto, para dictar un acto administrativo o expresar la voluntad de la Administración, con esta nueva regulación no se agotan las competencias estatales y autonómicas para establecer especialidades «ratione materiae» o para concretar ciertos extremos, como el órgano competente para resolver, sino que su carácter de común resulta de su aplicación a todas las Administraciones Públicas y respecto a todas sus actuaciones. Así lo ha venido reconociendo el Tribunal Constitucional en su jurisprudencia, al considerar que la regulación del procedimiento administrativo común por el Estado no obsta a que las Comunidades Autónomas dicten las normas de procedimiento necesarias para la aplicación de su Derecho

sustantivo, siempre que se respeten las reglas que, por ser competencia exclusiva del Estado, integran el concepto de Procedimiento Administrativo Común con carácter básico.

III

Son varios los antecedentes legislativos relevantes en esta materia. El legislador ha hecho evolucionar el concepto de procedimiento administrativo y adaptando la forma de actuación de las Administraciones al contexto histórico y la realidad social de cada momento. Al margen de la conocida como Ley de Azcárate, de 19 de octubre de 1889, la primera regulación completa del procedimiento administrativo en nuestro ordenamiento jurídico es la contenida en la Ley de Procedimiento Administrativo de 17 de julio de 1958.

La Constitución de 1978 alumbra un nuevo concepto de Administración, expresa y plenamente sometida a la Ley y al Derecho, como expresión democrática de la voluntad popular, y consagra su carácter instrumental, al ponerla al servicio objetivo de los intereses generales bajo la dirección del Gobierno, que responde políticamente por su gestión. En este sentido, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, supuso un hito clave de la evolución del Derecho administrativo en el nuevo marco constitucional. Para ello, incorporó avances significativos en las relaciones de las Administraciones con los administrados mediante la mejora del funcionamiento de aquellas y, sobre todo, a través de una mayor garantía de los derechos de los ciudadanos frente a la potestad de autotutela de la Administración, cuyo elemento de cierre se encuentra en la revisión judicial de su actuación por ministerio del artículo 106 del texto fundamental.

La Ley 4/1999, de 13 de enero, de modificación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, reformuló varios aspectos sustanciales del procedimiento administrativo, como el silencio administrativo, el sistema de revisión de actos administrativos o el régimen de responsabilidad patrimonial de las Administraciones, lo que permitió incrementar la seguridad jurídica de los interesados.

El desarrollo de las tecnologías de la información y comunicación también ha venido afectando profundamente a la forma y al contenido de las relaciones de la Administración con los ciudadanos y las empresas.

Si bien la Ley 30/1992, de 26 de noviembre, ya fue consciente del impacto de las nuevas tecnologías en las relaciones administrativas, fue la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, la que les dio carta de naturaleza legal, al establecer el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación de éstas de dotarse de los medios y sistemas necesarios para que ese derecho pudiera ejercerse. Sin embargo, en el entorno actual, la tramitación electrónica no puede ser todavía una forma especial de gestión de los procedimientos sino que debe constituir la actuación habitual de las Administraciones. Porque una Administración sin papel basada en un funcionamiento íntegramente electrónico no sólo sirve mejor a los principios de eficacia y eficiencia, al ahorrar costes a ciudadanos y empresas, sino que también refuerza las garantías de los interesados. En efecto, la constancia de documentos y actuaciones en un archivo electrónico facilita el cumplimiento de las obligaciones de transparencia, pues permite ofrecer información puntual, ágil y actualizada a los interesados.

Por otra parte, la regulación de esta materia venía adoleciendo de un problema de dispersión normativa y superposición de distintos regímenes jurídicos no siempre coherentes entre sí, de lo que es muestra la sucesiva aprobación de normas con incidencia en la materia, entre las que cabe citar: la Ley 17/2009, de 23 de noviembre, sobre libre acceso a las actividades de servicios y su ejercicio; la Ley 2/2011, de 4 de marzo, de Economía Sostenible; la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, o la Ley 20/2013, de 9 de diciembre, de garantía de la unidad de mercado.

Ante este escenario legislativo, resulta clave contar con una nueva Ley que sistematice toda la regulación relativa al procedimiento administrativo, que clarifique e integre el contenido de las citadas Ley 30/1992, de 26 de noviembre y Ley 11/2007, de 22 de junio, y profundice en la agilización de los procedimientos con un pleno funcionamiento electrónico.

Todo ello revertirá en un mejor cumplimiento de los principios constitucionales de eficacia y seguridad jurídica que deben regir la actuación de las Administraciones Públicas.

IV

Durante los más de veinte años de vigencia de la Ley 30/1992, de 26 de noviembre, en el seno de la Comisión Europea y de la Organización para la Cooperación y el Desarrollo Económicos se ha ido avanzando en la mejora de la producción normativa («Better regulation» y «Smart regulation»). Los diversos informes internacionales sobre la materia definen la regulación inteligente como un marco jurídico de calidad, que permite el cumplimiento de un objetivo regulatorio a la vez que ofrece los incentivos adecuados para dinamizar la actividad económica, permite simplificar procesos y reducir cargas administrativas. Para ello, resulta esencial un adecuado análisis de impacto de las normas de forma continua, tanto ex ante como ex post, así como la participación de los ciudadanos y empresas en los procesos de elaboración normativa, pues sobre ellos recae el cumplimiento de las leyes.

En la última década, la Ley 17/2009, de 23 de noviembre, y la Ley 2/2011, de 4 de marzo, supusieron un avance en la implantación de los principios de buena regulación, especialmente en lo referido al ejercicio de las actividades económicas. Ya en esta legislatura, la Ley 20/2013, de 9 de diciembre, ha dado importantes pasos adicionales, al poner a disposición de los ciudadanos la información con relevancia jurídica propia del procedimiento de elaboración de normas.

Sin embargo, es necesario contar con una nueva regulación que, terminando con la dispersión normativa existente, refuerce la participación ciudadana, la seguridad jurídica y la revisión del ordenamiento. Con estos objetivos, se establecen por primera vez en una ley las bases con arreglo a las cuales se ha de desenvolver la iniciativa legislativa y la potestad reglamentaria de las Administraciones Públicas con el objeto de asegurar su ejercicio de acuerdo con los principios de buena regulación, garantizar de modo adecuado la audiencia y participación de los ciudadanos en la elaboración de las normas y lograr la predictibilidad y evaluación pública del ordenamiento, como corolario imprescindible del derecho constitucional a la seguridad jurídica. Esta novedad deviene crucial especialmente en un Estado territorialmente descentralizado en el que coexisten tres niveles de Administración territorial que proyectan su actividad normativa sobre espacios subjetivos y geográficos en muchas ocasiones coincidentes. Con esta regulación se siguen las recomendaciones que en esta materia ha formulado la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en su informe emitido en 2014 «Spain: From Administrative Reform to Continous Improvement».

V

La Ley se estructura en 133 artículos, distribuidos en siete títulos, cinco disposiciones adicionales, cinco disposiciones transitorias, una disposición derogatoria y siete disposiciones finales.

El título preliminar, de disposiciones generales, aborda el ámbito objetivo y subjetivo de la Ley. Entre sus principales novedades, cabe señalar, la inclusión en el objeto de la Ley, con carácter básico, de los principios que informan el ejercicio de la iniciativa legislativa y la potestad reglamentaria de las Administraciones. Se prevé la aplicación de lo previsto en esta Ley a todos los sujetos comprendidos en el concepto de Sector Público, si bien las Corporaciones de Derecho Público se regirán por su normativa específica en el ejercicio de las funciones públicas que les hayan sido atribuidas y supletoriamente por la presente Ley.

Asimismo, destaca la previsión de que sólo mediante Ley puedan establecerse trámites adicionales o distintos a los contemplados en esta norma, pudiéndose concretar reglamentariamente ciertas especialidades del procedimiento referidas a la identificación de los órganos competentes, plazos, formas de iniciación y terminación, publicación e informes a recabar. Esta previsión no afecta a los trámites adicionales o distintos ya recogidos en las leyes especiales vigentes, ni a la concreción que, en normas reglamentarias, se haya producido de los órganos competentes, los plazos propios del concreto procedimiento por razón de la materia, las formas de iniciación y terminación, la publicación de los actos o los

informes a recabar, que mantendrán sus efectos. Así, entre otros casos, cabe señalar la vigencia del anexo 2 al que se refiere la disposición adicional vigésima novena de la Ley 14/2000, de 29 de diciembre, de medidas fiscales, administrativas y del orden social, que establece una serie de procedimientos que quedan excepcionados de la regla general del silencio administrativo positivo.

El título I, de los interesados en el procedimiento, regula entre otras cuestiones, las especialidades de la capacidad de obrar en el ámbito del Derecho administrativo, haciéndola extensiva por primera vez a los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos cuando la Ley así lo declare expresamente. En materia de representación, se incluyen nuevos medios para acreditarla en el ámbito exclusivo de las Administraciones Públicas, como son el apoderamiento «apud acta», presencial o electrónico, o la acreditación de su inscripción en el registro electrónico de apoderamientos de la Administración Pública u Organismo competente. Igualmente, se dispone la obligación de cada Administración Pública de contar con un registro electrónico de apoderamientos, pudiendo las Administraciones territoriales adherirse al del Estado, en aplicación del principio de eficiencia, reconocido en el artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Por otro lado, este título dedica parte de su articulado a una de las novedades más importantes de la Ley: la separación entre identificación y firma electrónica y la simplificación de los medios para acreditar una u otra, de modo que, con carácter general, sólo será necesaria la primera, y se exigirá la segunda cuando deba acreditarse la voluntad y consentimiento del interesado. Se establece, con carácter básico, un conjunto mínimo de categorías de medios de identificación y firma a utilizar por todas las Administraciones. En particular, se admitirán como sistemas de firma: los sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica, que comprenden tanto los certificados electrónicos de persona jurídica como los de entidad sin personalidad jurídica; los sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados cualificados de sello electrónico; así como cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan. Se admitirán como sistemas de identificación cualquiera de los sistemas de firma admitidos, así como sistemas de clave concertada y cualquier otro que establezcan las Administraciones Públicas.

Tanto los sistemas de identificación como los de firma previstos en esta Ley son plenamente coherentes con lo dispuesto en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. Debe recordarse la obligación de los Estados miembros de admitir los sistemas de identificación electrónica notificados a la Comisión Europea por el resto de Estados miembros, así como los sistemas de firma y sello electrónicos basados en certificados electrónicos cualificados emitidos por prestadores de servicios que figuren en las listas de confianza de otros Estados miembros de la Unión Europea, en los términos que prevea dicha norma comunitaria.

El título II, de la actividad de las Administraciones Públicas, se estructura en dos capítulos. El capítulo I sobre normas generales de actuación identifica como novedad, los sujetos obligados a relacionarse electrónicamente con las Administraciones Públicas.

Asimismo, en el citado Capítulo se dispone la obligación de todas las Administraciones Públicas de contar con un registro electrónico general, o, en su caso, adherirse al de la Administración General del Estado. Estos registros estarán asistidos a su vez por la actual red de oficinas en materia de registros, que pasarán a denominarse oficinas de asistencia en materia de registros, y que permitirán a los interesados, en el caso que así lo deseen, presentar sus solicitudes en papel, las cuales se convertirán a formato electrónico.

En materia de archivos se introduce como novedad la obligación de cada Administración Pública de mantener un archivo electrónico único de los documentos que correspondan a procedimientos finalizados, así como la obligación de que estos expedientes sean conservados en un formato que permita garantizar la autenticidad, integridad y conservación del documento.

A este respecto, cabe señalar que la creación de este archivo electrónico único resultará compatible con los diversos sistemas y redes de archivos en los términos previstos en la legislación vigente, y respetará el reparto de responsabilidades sobre la custodia o traspaso correspondiente. Asimismo, el archivo electrónico único resultará compatible con la continuidad del Archivo Histórico Nacional de acuerdo con lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español y su normativa de desarrollo.

Igualmente, en el capítulo I se regula el régimen de validez y eficacia de las copias, en donde se aclara y simplifica el actual régimen y se definen los requisitos necesarios para que una copia sea auténtica, las características que deben reunir los documentos emitidos por las Administraciones Públicas para ser considerados válidos, así como los que deben aportar los interesados al procedimiento, estableciendo con carácter general la obligación de las Administraciones Públicas de no requerir documentos ya aportados por los interesados, elaborados por las Administraciones Públicas o documentos originales, salvo las excepciones contempladas en la Ley. Por tanto, el interesado podrá presentar con carácter general copias de documentos, ya sean digitalizadas por el propio interesado o presentadas en soporte papel.

Destaca asimismo, la obligación de las Administraciones Públicas de contar con un registro u otro sistema equivalente que permita dejar constancia de los funcionarios habilitados para la realización de copias auténticas, de forma que se garantice que las mismas han sido expedidas adecuadamente, y en el que, si así decide organizarlo cada Administración, podrán constar también conjuntamente los funcionarios dedicados a asistir a los interesados en el uso de medios electrónicos, no existiendo impedimento a que un mismo funcionario tenga reconocida ambas funciones o sólo una de ellas.

El capítulo II, de términos y plazos, establece las reglas para su cómputo, ampliación o la tramitación de urgencia. Como principal novedad destaca la introducción del cómputo de plazos por horas y la declaración de los sábados como días inhábiles, unificando de este modo el cómputo de plazos en el ámbito judicial y el administrativo.

El título III, de los actos administrativos, se estructura en tres capítulos y se centra en la regulación de los requisitos de los actos administrativos, su eficacia y las reglas sobre nulidad y anulabilidad, manteniendo en su gran mayoría las reglas generales ya establecidas por la Ley 30/1992, de 26 de noviembre.

Merecen una mención especial las novedades introducidas en materia de notificaciones electrónicas, que serán preferentes y se realizarán en la sede electrónica o en la dirección electrónica habilitada única, según corresponda. Asimismo, se incrementa la seguridad jurídica de los interesados estableciendo nuevas medidas que garanticen el conocimiento de la puesta a disposición de las notificaciones como: el envío de avisos de notificación, siempre que esto sea posible, a los dispositivos electrónicos y/o a la dirección de correo electrónico que el interesado haya comunicado, así como el acceso a sus notificaciones a través del Punto de Acceso General Electrónico de la Administración que funcionará como un portal de entrada.

El título IV, de disposiciones sobre el procedimiento administrativo común, se estructura en siete capítulos y entre sus principales novedades destaca que los anteriores procedimientos especiales sobre potestad sancionadora y responsabilidad patrimonial que la Ley 30/1992, de 26 de noviembre, regulaba en títulos separados, ahora se han integrado como especialidades del procedimiento administrativo común. Este planteamiento responde a uno de los objetivos que persigue esta Ley, la simplificación de los procedimientos administrativos y su integración como especialidades en el procedimiento administrativo común, contribuyendo así a aumentar la seguridad jurídica. De acuerdo con la sistemática seguida, los principios generales de la potestad sancionadora y de la responsabilidad patrimonial de las Administraciones Públicas, en cuanto que atañen a aspectos más orgánicos que procedimentales, se regulan en la Ley de Régimen Jurídico del Sector Público.

Asimismo, este título incorpora a las fases de iniciación, ordenación, instrucción y finalización del procedimiento el uso generalizado y obligatorio de medios electrónicos. Igualmente, se incorpora la regulación del expediente administrativo estableciendo su formato electrónico y los documentos que deben integrarlo.

Como novedad dentro de este título, se incorpora un nuevo Capítulo relativo a la tramitación simplificada del procedimiento administrativo común, donde se establece su ámbito objetivo de aplicación, el plazo máximo de resolución que será de treinta días y los trámites de que constará. Si en un procedimiento fuera necesario realizar cualquier otro trámite adicional, deberá seguirse entonces la tramitación ordinaria. Asimismo, cuando en un procedimiento tramitado de manera simplificada fuera preceptiva la emisión del Dictamen del Consejo de Estado, u órgano consultivo equivalente, y éste manifestara un criterio contrario al fondo de la propuesta de resolución, para mayor garantía de los interesados se deberá continuar el procedimiento pero siguiendo la tramitación ordinaria, no ya la abreviada, pudiéndose en este caso realizar otros trámites no previstos en el caso de la tramitación simplificada, como la realización de pruebas a solicitud de los interesados. Todo ello, sin perjuicio de la posibilidad de acordar la tramitación de urgencia del procedimiento en los mismos términos que ya contemplaba la Ley 30/1992, de 26 de noviembre.

El título V, de la revisión de los actos en vía administrativa, mantiene las mismas vías previstas en la Ley 30/1992, de 26 de noviembre, permaneciendo por tanto la revisión de oficio y la tipología de recursos administrativos existentes hasta la fecha (alzada, potestativo de reposición y extraordinario de revisión). No obstante, cabe destacar como novedad la posibilidad de que cuando una Administración deba resolver una pluralidad de recursos administrativos que traigan causa de un mismo acto administrativo y se hubiera interpuesto un recurso judicial contra una resolución administrativa o contra el correspondiente acto presunto desestimatorio, el órgano administrativo podrá acordar la suspensión del plazo para resolver hasta que recaiga pronunciamiento judicial.

De acuerdo con la voluntad de suprimir trámites que, lejos de constituir una ventaja para los administrados, suponían una carga que dificultaba el ejercicio de sus derechos, la Ley no contempla ya las reclamaciones previas en vía civil y laboral, debido a la escasa utilidad práctica que han demostrado hasta la fecha y que, de este modo, quedan suprimidas.

El título VI, sobre la iniciativa legislativa y potestad normativa de las Administraciones Públicas, recoge los principios a los que ha de ajustar su ejercicio la Administración titular, haciendo efectivos los derechos constitucionales en este ámbito.

Junto con algunas mejoras en la regulación vigente sobre jerarquía, publicidad de las normas y principios de buena regulación, se incluyen varias novedades para incrementar la participación de los ciudadanos en el procedimiento de elaboración de normas, entre las que destaca, la necesidad de recabar, con carácter previo a la elaboración de la norma, la opinión de ciudadanos y empresas acerca de los problemas que se pretenden solucionar con la iniciativa, la necesidad y oportunidad de su aprobación, los objetivos de la norma y las posibles soluciones alternativas regulatorias y no regulatorias.

Por otra parte, en aras de una mayor seguridad jurídica, y la predictibilidad del ordenamiento, se apuesta por mejorar la planificación normativa ex ante. Para ello, todas las Administraciones divulgarán un Plan Anual Normativo en el que se recogerán todas las propuestas con rango de ley o de reglamento que vayan a ser elevadas para su aprobación el año siguiente. Al mismo tiempo, se fortalece la evaluación ex post, puesto que junto con el deber de revisar de forma continua la adaptación de la normativa a los principios de buena regulación, se impone la obligación de evaluar periódicamente la aplicación de las normas en vigor, con el objeto de comprobar si han cumplido los objetivos perseguidos y si el coste y cargas derivados de ellas estaba justificado y adecuadamente valorado.

Por lo que respecta a las disposiciones adicionales, transitorias, derogatorias y finales, cabe aludir a la relativa a la adhesión por parte de las Comunidades Autónomas y Entidades Locales a los registros y sistemas establecidos por la Administración General del Estado en aplicación del principio de eficiencia reconocido en la Ley Orgánica 2/2012, de 27 de abril.

Destaca igualmente, la disposición sobre las especialidades por razón de la materia donde se establece una serie de actuaciones y procedimientos que se regirán por su normativa específica y supletoriamente por lo previsto en esta Ley, entre las que cabe destacar las de aplicación de los tributos y revisión en materia tributaria y aduanera, las de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y Desempleo, en donde se entienden comprendidos, entre otros, los actos de encuadramiento y afiliación de la Seguridad Social y las aportaciones económicas por despidos que afecten a trabajadores de cincuenta o más años en empresas con beneficios,

así como las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.

Por último, la Ley contiene las disposiciones de derecho transitorio aplicables a los procedimientos en curso, a su entrada en vigor, a archivos y registros y al Punto de Acceso General electrónico, así como las que habilitan para el desarrollo de lo previsto en la Ley.

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. La presente Ley tiene por objeto regular los requisitos de validez y eficacia de los actos administrativos, el procedimiento administrativo común a todas las Administraciones Públicas, incluyendo el sancionador y el de reclamación de responsabilidad de las Administraciones Públicas, así como los principios a los que se ha de ajustar el ejercicio de la iniciativa legislativa y la potestad reglamentaria.

2. Solo mediante ley, cuando resulte eficaz, proporcionado y necesario para la consecución de los fines propios del procedimiento, y de manera motivada, podrán incluirse trámites adicionales o distintos a los contemplados en esta Ley. Reglamentariamente podrán establecerse especialidades del procedimiento referidas a los órganos competentes, plazos propios del concreto procedimiento por razón de la materia, formas de iniciación y terminación, publicación e informes a recabar.

Artículo 2. *Ámbito subjetivo de aplicación.*

1. La presente Ley se aplica al sector público, que comprende:

a) La Administración General del Estado.
b) Las Administraciones de las Comunidades Autónomas.
c) Las Entidades que integran la Administración Local.
d) El sector público institucional.

2. El sector público institucional se integra por:

a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.

b) Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas, que quedarán sujetas a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, y en todo caso, cuando ejerzan potestades administrativas.

c) Las Universidades públicas, que se regirán por su normativa específica y supletoriamente por las previsiones de esta Ley.

3. Tienen la consideración de Administraciones Públicas la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2 anterior.

4. Las Corporaciones de Derecho Público se regirán por su normativa específica en el ejercicio de las funciones públicas que les hayan sido atribuidas por Ley o delegadas por una Administración Pública, y supletoriamente por la presente Ley.

TÍTULO I

De los interesados en el procedimiento

CAPÍTULO I

La capacidad de obrar y el concepto de interesado

Artículo 3. *Capacidad de obrar.*

A los efectos previstos en esta Ley, tendrán capacidad de obrar ante las Administraciones Públicas:

a) Las personas físicas o jurídicas que ostenten capacidad de obrar con arreglo a las normas civiles.

b) Los menores de edad para el ejercicio y defensa de aquellos de sus derechos e intereses cuya actuación esté permitida por el ordenamiento jurídico sin la asistencia de la persona que ejerza la patria potestad, tutela o curatela. Se exceptúa el supuesto de los menores incapacitados, cuando la extensión de la incapacitación afecte al ejercicio y defensa de los derechos o intereses de que se trate.

c) Cuando la Ley así lo declare expresamente, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos.

Artículo 4. *Concepto de interesado.*

1. Se consideran interesados en el procedimiento administrativo:

a) Quienes lo promuevan como titulares de derechos o intereses legítimos individuales o colectivos.

b) Los que, sin haber iniciado el procedimiento, tengan derechos que puedan resultar afectados por la decisión que en el mismo se adopte.

c) Aquellos cuyos intereses legítimos, individuales o colectivos, puedan resultar afectados por la resolución y se personen en el procedimiento en tanto no haya recaído resolución definitiva.

2. Las asociaciones y organizaciones representativas de intereses económicos y sociales serán titulares de intereses legítimos colectivos en los términos que la Ley reconozca.

3. Cuando la condición de interesado derivase de alguna relación jurídica transmisible, el derecho-habiente sucederá en tal condición cualquiera que sea el estado del procedimiento.

Artículo 5. *Representación.*

1. Los interesados con capacidad de obrar podrán actuar por medio de representante, entendiéndose con éste las actuaciones administrativas, salvo manifestación expresa en contra del interesado.

2. Las personas físicas con capacidad de obrar y las personas jurídicas, siempre que ello esté previsto en sus Estatutos, podrán actuar en representación de otras ante las Administraciones Públicas.

3. Para formular solicitudes, presentar declaraciones responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos en nombre de otra persona, deberá acreditarse la representación. Para los actos y gestiones de mero trámite se presumirá aquella representación.

4. La representación podrá acreditarse mediante cualquier medio válido en Derecho que deje constancia fidedigna de su existencia.

A estos efectos, se entenderá acreditada la representación realizada mediante apoderamiento apud acta efectuado por comparecencia personal o comparecencia electrónica en la correspondiente sede electrónica, o a través de la acreditación de su inscripción en el registro electrónico de apoderamientos de la Administración Pública competente.

5. El órgano competente para la tramitación del procedimiento deberá incorporar al expediente administrativo acreditación de la condición de representante y de los poderes que tiene reconocidos en dicho momento. El documento electrónico que acredite el resultado de la consulta al registro electrónico de apoderamientos correspondiente tendrá la condición de acreditación a estos efectos.

6. La falta o insuficiente acreditación de la representación no impedirá que se tenga por realizado el acto de que se trate, siempre que se aporte aquélla o se subsane el defecto dentro del plazo de diez días que deberá conceder al efecto el órgano administrativo, o de un plazo superior cuando las circunstancias del caso así lo requieran.

7. Las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de los interesados. Dicha habilitación deberá especificar las condiciones y obligaciones a las que se comprometen los que así adquieran la condición de representantes, y determinará la presunción de validez de la representación salvo que la normativa de aplicación prevea otra cosa. Las Administraciones Públicas podrán requerir, en cualquier momento, la acreditación de dicha representación. No obstante, siempre podrá comparecer el interesado por sí mismo en el procedimiento.

Artículo 6. *Registros electrónicos de apoderamientos.*

1. La Administración General del Estado, las Comunidades Autónomas y las Entidades Locales dispondrán de un registro electrónico general de apoderamientos, en el que deberán inscribirse, al menos, los de carácter general otorgados apud acta, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo a favor de representante, para actuar en su nombre ante las Administraciones Públicas. También deberá constar el bastanteo realizado del poder.

En el ámbito estatal, este registro será el Registro Electrónico de Apoderamientos de la Administración General del Estado.

Los registros generales de apoderamientos no impedirán la existencia de registros particulares en cada Organismo donde se inscriban los poderes otorgados para la realización de trámites específicos en el mismo. Cada Organismo podrá disponer de su propio registro electrónico de apoderamientos.

2. Los registros electrónicos generales y particulares de apoderamientos pertenecientes a todas y cada una de las Administraciones, deberán ser plenamente interoperables entre sí, de modo que se garantice su interconexión, compatibilidad informática, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se incorporen a los mismos.

Los registros electrónicos generales y particulares de apoderamientos permitirán comprobar válidamente la representación de quienes actúen ante las Administraciones Públicas en nombre de un tercero, mediante la consulta a otros registros administrativos similares, al registro mercantil, de la propiedad, y a los protocolos notariales.

Los registros mercantiles, de la propiedad, y de los protocolos notariales serán interoperables con los registros electrónicos generales y particulares de apoderamientos.

3. Los asientos que se realicen en los registros electrónicos generales y particulares de apoderamientos deberán contener, al menos, la siguiente información:

a) Nombre y apellidos o la denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del poderdante.

b) Nombre y apellidos o la denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del apoderado.

c) Fecha de inscripción.

d) Período de tiempo por el cual se otorga el poder.

e) Tipo de poder según las facultades que otorgue.

4. Los poderes que se inscriban en los registros electrónicos generales y particulares de apoderamientos deberán corresponder a alguna de las siguientes tipologías:

a) Un poder general para que el apoderado pueda actuar en nombre del poderdante en cualquier actuación administrativa y ante cualquier Administración.

b) Un poder para que el apoderado pueda actuar en nombre del poderdante en cualquier actuación administrativa ante una Administración u Organismo concreto.

c) Un poder para que el apoderado pueda actuar en nombre del poderdante únicamente para la realización de determinados trámites especificados en el poder.

(Párrafo anulado)

Cada Comunidad Autónoma aprobará los modelos de poderes inscribibles en el registro cuando se circunscriba a actuaciones ante su respectiva Administración.

5. El apoderamiento «*apud* acta» se otorgará mediante comparecencia electrónica en la correspondiente sede electrónica haciendo uso de los sistemas de firma electrónica previstos en esta Ley, o bien mediante comparecencia personal en las oficinas de asistencia en materia de registros.

6. Los poderes inscritos en el registro tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción. En todo caso, en cualquier momento antes de la finalización de dicho plazo el poderdante podrá revocar o prorrogar el poder. Las prórrogas otorgadas por el poderdante al registro tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción.

7. Las solicitudes de inscripción del poder, de revocación, de prórroga o de denuncia del mismo podrán dirigirse a cualquier registro, debiendo quedar inscrita esta circunstancia en el registro de la Administración u Organismo ante la que tenga efectos el poder y surtiendo efectos desde la fecha en la que se produzca dicha inscripción.

Artículo 7. *Pluralidad de interesados.*

Cuando en una solicitud, escrito o comunicación figuren varios interesados, las actuaciones a que den lugar se efectuarán con el representante o el interesado que expresamente hayan señalado, y, en su defecto, con el que figure en primer término.

Artículo 8. *Nuevos interesados en el procedimiento.*

Si durante la instrucción de un procedimiento que no haya tenido publicidad, se advierte la existencia de personas que sean titulares de derechos o intereses legítimos y directos cuya identificación resulte del expediente y que puedan resultar afectados por la resolución que se dicte, se comunicará a dichas personas la tramitación del procedimiento.

CAPÍTULO II

Identificación y firma de los interesados en el procedimiento administrativo

Artículo 9. *Sistemas de identificación de los interesados en el procedimiento.*

1. Las Administraciones Públicas están obligadas a verificar la identidad de los interesados en el procedimiento administrativo, mediante la comprobación de su nombre y apellidos o denominación o razón social, según corresponda, que consten en el Documento Nacional de Identidad o documento identificativo equivalente.

2. Los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas siguientes:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los

cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

3. En relación con los sistemas de identificación previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo.

Artículo 10. *Sistemas de firma admitidos por las Administraciones Públicas.*

1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la ‘‘Lista de confianza de prestadores de servicios de certificación’’.

c) Cualquier otro sistema que las Administraciones públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad y previa comunicación a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Esta comunicación vendrá acompañada de una declaración responsable de que se cumple con todos los requisitos establecidos en la normativa vigente. De forma previa a la eficacia jurídica del sistema, habrán de transcurrir dos meses desde dicha comunicación, durante los cuales el órgano estatal competente por motivos de seguridad pública podrá acudir a la vía jurisdiccional, previo informe vinculante de la Secretaría de Estado de Seguridad, que deberá emitir en el plazo de diez días desde su solicitud.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

3. En relación con los sistemas de firma previstos en la letra c) del apartado anterior, se establece la obligatoriedad de que los recursos técnicos necesarios para la recogida, almacenamiento, tratamiento y gestión de dichos sistemas se encuentren situados en territorio de la Unión Europea, y en caso de tratarse de categorías especiales de datos a los que se refiere el artículo 9 del Reglamento (UE) 2016/679, del Parlamento Europeo y del

Consejo, de 27 de abril de 2016, en territorio español. En cualquier caso, los datos se encontrarán disponibles para su acceso por parte de las autoridades judiciales y administrativas competentes.

Los datos a que se refiere el párrafo anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

4. Cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

5. Cuando los interesados utilicen un sistema de firma de los previstos en este artículo, su identidad se entenderá ya acreditada mediante el propio acto de la firma.

Artículo 11. *Uso de medios de identificación y firma en el procedimiento administrativo.*

1. Con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo, será suficiente con que los interesados acrediten previamente su identidad a través de cualquiera de los medios de identificación previstos en esta Ley.

2. Las Administraciones Públicas sólo requerirán a los interesados el uso obligatorio de firma para:

a) Formular solicitudes.
b) Presentar declaraciones responsables o comunicaciones.
c) Interponer recursos.
d) Desistir de acciones.
e) Renunciar a derechos.

Artículo 12. *Asistencia en el uso de medios electrónicos a los interesados.*

1. Las Administraciones Públicas deberán garantizar que los interesados pueden relacionarse con la Administración a través de medios electrónicos, para lo que pondrán a su disposición los canales de acceso que sean necesarios así como los sistemas y aplicaciones que en cada caso se determinen.

2. Las Administraciones Públicas asistirán en el uso de medios electrónicos a los interesados no incluidos en los apartados 2 y 3 del artículo 14 que así lo soliciten, especialmente en lo referente a la identificación y firma electrónica, presentación de solicitudes a través del registro electrónico general y obtención de copias auténticas.

Asimismo, si alguno de estos interesados no dispone de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por un funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado que carezca de los medios electrónicos necesarios se identifique ante el funcionario y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia para los casos de discrepancia o litigio.

3. La Administración General del Estado, las Comunidades Autónomas y las Entidades Locales mantendrán actualizado un registro, u otro sistema equivalente, donde constarán los funcionarios habilitados para la identificación o firma regulada en este artículo. Estos registros o sistemas deberán ser plenamente interoperables y estar interconectados con los de las restantes Administraciones Públicas, a los efectos de comprobar la validez de las citadas habilitaciones.

En este registro o sistema equivalente, al menos, constarán los funcionarios que presten servicios en las oficinas de asistencia en materia de registros.

TÍTULO II

De la actividad de las Administraciones Públicas

CAPÍTULO I

Normas generales de actuación

Artículo 13. *Derechos de las personas en sus relaciones con las Administraciones Públicas.*

Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos:

a) A comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración.
b) A ser asistidos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas.
c) A utilizar las lenguas oficiales en el territorio de su Comunidad Autónoma, de acuerdo con lo previsto en esta Ley y en el resto del ordenamiento jurídico.
d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.
e) A ser tratados con respeto y deferencia por las autoridades y empleados públicos, que habrán de facilitarles el ejercicio de sus derechos y el cumplimiento de sus obligaciones.
f) A exigir las responsabilidades de las Administraciones Públicas y autoridades, cuando así corresponda legalmente.
g) A la obtención y utilización de los medios de identificación y firma electrónica contemplados en esta Ley.
h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

Estos derechos se entienden sin perjuicio de los reconocidos en el artículo 53 referidos a los interesados en el procedimiento administrativo.

Artículo 14. *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Las personas físicas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas. El medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento.
2. En todo caso, estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los siguientes sujetos:

a) Las personas jurídicas.
b) Las entidades sin personalidad jurídica.
c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria, para los trámites y actuaciones que realicen con las Administraciones Públicas en ejercicio de dicha actividad profesional. En todo caso, dentro de este colectivo se entenderán incluidos los notarios y registradores de la propiedad y mercantiles.
d) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración.
e) Los empleados de las Administraciones Públicas para los trámites y actuaciones que realicen con ellas por razón de su condición de empleado público, en la forma en que se determine reglamentariamente por cada Administración.

3. Reglamentariamente, las Administraciones podrán establecer la obligación de relacionarse con ellas a través de medios electrónicos para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

Artículo 15. *Lengua de los procedimientos.*

1. La lengua de los procedimientos tramitados por la Administración General del Estado será el castellano. No obstante lo anterior, los interesados que se dirijan a los órganos de la Administración General del Estado con sede en el territorio de una Comunidad Autónoma podrán utilizar también la lengua que sea cooficial en ella.

En este caso, el procedimiento se tramitará en la lengua elegida por el interesado. Si concurrieran varios interesados en el procedimiento, y existiera discrepancia en cuanto a la lengua, el procedimiento se tramitará en castellano, si bien los documentos o testimonios que requieran los interesados se expedirán en la lengua elegida por los mismos.

2. En los procedimientos tramitados por las Administraciones de las Comunidades Autónomas y de las Entidades Locales, el uso de la lengua se ajustará a lo previsto en la legislación autonómica correspondiente.

3. La Administración Pública instructora deberá traducir al castellano los documentos, expedientes o partes de los mismos que deban surtir efecto fuera del territorio de la Comunidad Autónoma y los documentos dirigidos a los interesados que así lo soliciten expresamente. Si debieran surtir efectos en el territorio de una Comunidad Autónoma donde sea cooficial esa misma lengua distinta del castellano, no será precisa su traducción.

Artículo 16. *Registros.*

1. Cada Administración dispondrá de un Registro Electrónico General, en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, Organismo público o Entidad vinculado o dependiente a éstos. También se podrán anotar en el mismo, la salida de los documentos oficiales dirigidos a otros órganos o particulares.

Los Organismos públicos vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende.

El Registro Electrónico General de cada Administración funcionará como un portal que facilitará el acceso a los registros electrónicos de cada Organismo. Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

Las disposiciones de creación de los registros electrónicos se publicarán en el diario oficial correspondiente y su texto íntegro deberá estar disponible para consulta en la sede electrónica de acceso al registro. En todo caso, las disposiciones de creación de registros electrónicos especificarán el órgano o unidad responsable de su gestión, así como la fecha y hora oficial y los días declarados como inhábiles.

En la sede electrónica de acceso a cada registro figurará la relación actualizada de trámites que pueden iniciarse en el mismo.

2. Los asientos se anotarán respetando el orden temporal de recepción o salida de los documentos, e indicarán la fecha del día en que se produzcan. Concluido el trámite de registro, los documentos serán cursados sin dilación a sus destinatarios y a las unidades administrativas correspondientes desde el registro en que hubieran sido recibidas.

3. El registro electrónico de cada Administración u Organismo garantizará la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación del interesado, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra. Para ello, se emitirá automáticamente un recibo consistente en una copia autenticada del documento de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro, así como un recibo acreditativo de

otros documentos que, en su caso, lo acompañen, que garantice la integridad y el no repudio de los mismos.

4. Los documentos que los interesados dirijan a los órganos de las Administraciones Públicas podrán presentarse:

a) En el registro electrónico de la Administración u Organismo al que se dirijan, así como en los restantes registros electrónicos de cualquiera de los sujetos a los que se refiere el artículo 2.1.

b) En las oficinas de Correos, en la forma que reglamentariamente se establezca.

c) En las representaciones diplomáticas u oficinas consulares de España en el extranjero.

d) En las oficinas de asistencia en materia de registros.

e) En cualquier otro que establezcan las disposiciones vigentes.

Los registros electrónicos de todas y cada una de las Administraciones, deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de los asientos registrales y de los documentos que se presenten en cualquiera de los registros.

5. Los documentos presentados de manera presencial ante las Administraciones Públicas, deberán ser digitalizados, de acuerdo con lo previsto en el artículo 27 y demás normativa aplicable, por la oficina de asistencia en materia de registros en la que hayan sido presentados para su incorporación al expediente administrativo electrónico, devolviéndose los originales al interesado, sin perjuicio de aquellos supuestos en que la norma determine la custodia por la Administración de los documentos presentados o resulte obligatoria la presentación de objetos o de documentos en un soporte específico no susceptibles de digitalización.

Reglamentariamente, las Administraciones podrán establecer la obligación de presentar determinados documentos por medios electrónicos para ciertos procedimientos y colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

6. Podrán hacerse efectivos mediante transferencia dirigida a la oficina pública correspondiente cualesquiera cantidades que haya que satisfacer en el momento de la presentación de documentos a las Administraciones Públicas, sin perjuicio de la posibilidad de su abono por otros medios.

7. Las Administraciones Públicas deberán hacer pública y mantener actualizada una relación de las oficinas en las que se prestará asistencia para la presentación electrónica de documentos.

8. No se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación.

Artículo 17. *Archivo de documentos.*

1. Cada Administración deberá mantener un archivo electrónico único de los documentos electrónicos que correspondan a procedimientos finalizados, en los términos establecidos en la normativa reguladora aplicable.

2. Los documentos electrónicos deberán conservarse en un formato que permita garantizar la autenticidad, integridad y conservación del documento, así como su consulta con independencia del tiempo transcurrido desde su emisión. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones. La eliminación de dichos documentos deberá ser autorizada de acuerdo a lo dispuesto en la normativa aplicable.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Artículo 18. *Colaboración de las personas.*

1. Las personas colaborarán con la Administración en los términos previstos en la Ley que en cada caso resulte aplicable, y a falta de previsión expresa, facilitarán a la Administración los informes, inspecciones y otros actos de investigación que requieran para el ejercicio de sus competencias, salvo que la revelación de la información solicitada por la Administración atentara contra el honor, la intimidad personal o familiar o supusieran la comunicación de datos confidenciales de terceros de los que tengan conocimiento por la prestación de servicios profesionales de diagnóstico, asesoramiento o defensa, sin perjuicio de lo dispuesto en la legislación en materia de blanqueo de capitales y financiación de actividades terroristas.

2. Los interesados en un procedimiento que conozcan datos que permitan identificar a otros interesados que no hayan comparecido en él tienen el deber de proporcionárselos a la Administración actuante.

3. Cuando las inspecciones requieran la entrada en el domicilio del afectado o en los restantes lugares que requieran autorización del titular, se estará a lo dispuesto en el artículo 100.

Artículo 19. *Comparecencia de las personas.*

1. La comparecencia de las personas ante las oficinas públicas, ya sea presencialmente o por medios electrónicos, sólo será obligatoria cuando así esté previsto en una norma con rango de ley.

2. En los casos en que proceda la comparecencia, la correspondiente citación hará constar expresamente el lugar, fecha, hora, los medios disponibles y objeto de la comparecencia, así como los efectos de no atenderla.

3. Las Administraciones Públicas entregarán al interesado certificación acreditativa de la comparecencia cuando así lo solicite.

Artículo 20. *Responsabilidad de la tramitación.*

1. Los titulares de las unidades administrativas y el personal al servicio de las Administraciones Públicas que tuviesen a su cargo la resolución o el despacho de los asuntos, serán responsables directos de su tramitación y adoptarán las medidas oportunas para remover los obstáculos que impidan, dificulten o retrasen el ejercicio pleno de los derechos de los interesados o el respeto a sus intereses legítimos, disponiendo lo necesario para evitar y eliminar toda anormalidad en la tramitación de procedimientos.

2. Los interesados podrán solicitar la exigencia de esa responsabilidad a la Administración Pública de que dependa el personal afectado.

Artículo 21. *Obligación de resolver.*

1. La Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación.

En los casos de prescripción, renuncia del derecho, caducidad del procedimiento o desistimiento de la solicitud, así como de desaparición sobrevenida del objeto del procedimiento, la resolución consistirá en la declaración de la circunstancia que concurra en cada caso, con indicación de los hechos producidos y las normas aplicables.

Se exceptúan de la obligación a que se refiere el párrafo primero, los supuestos de terminación del procedimiento por pacto o convenio, así como los procedimientos relativos al ejercicio de derechos sometidos únicamente al deber de declaración responsable o comunicación a la Administración.

2. El plazo máximo en el que debe notificarse la resolución expresa será el fijado por la norma reguladora del correspondiente procedimiento.

Este plazo no podrá exceder de seis meses salvo que una norma con rango de Ley establezca uno mayor o así venga previsto en el Derecho de la Unión Europea.

3. Cuando las normas reguladoras de los procedimientos no fijen el plazo máximo, éste será de tres meses. Este plazo y los previstos en el apartado anterior se contarán:

a) En los procedimientos iniciados de oficio, desde la fecha del acuerdo de iniciación.

b) En los iniciados a solicitud del interesado, desde la fecha en que la solicitud haya tenido entrada en el registro electrónico de la Administración u Organismo competente para su tramitación.

4. Las Administraciones Públicas deben publicar y mantener actualizadas en el portal web, a efectos informativos, las relaciones de procedimientos de su competencia, con indicación de los plazos máximos de duración de los mismos, así como de los efectos que produzca el silencio administrativo.

En todo caso, las Administraciones Públicas informarán a los interesados del plazo máximo establecido para la resolución de los procedimientos y para la notificación de los actos que les pongan término, así como de los efectos que pueda producir el silencio administrativo. Dicha mención se incluirá en la notificación o publicación del acuerdo de iniciación de oficio, o en la comunicación que se dirigirá al efecto al interesado dentro de los diez días siguientes a la recepción de la solicitud iniciadora del procedimiento en el registro electrónico de la Administración u Organismo competente para su tramitación. En este último caso, la comunicación indicará además la fecha en que la solicitud ha sido recibida por el órgano competente.

5. Cuando el número de las solicitudes formuladas o las personas afectadas pudieran suponer un incumplimiento del plazo máximo de resolución, el órgano competente para resolver, a propuesta razonada del órgano instructor, o el superior jerárquico del órgano competente para resolver, a propuesta de éste, podrán habilitar los medios personales y materiales para cumplir con el despacho adecuado y en plazo.

6. El personal al servicio de las Administraciones Públicas que tenga a su cargo el despacho de los asuntos, así como los titulares de los órganos administrativos competentes para instruir y resolver son directamente responsables, en el ámbito de sus competencias, del cumplimiento de la obligación legal de dictar resolución expresa en plazo.

El incumplimiento de dicha obligación dará lugar a la exigencia de responsabilidad disciplinaria, sin perjuicio de la que hubiere lugar de acuerdo con la normativa aplicable.

Artículo 22. *Suspensión del plazo máximo para resolver.*

1. El transcurso del plazo máximo legal para resolver un procedimiento y notificar la resolución se podrá suspender en los siguientes casos:

a) Cuando deba requerirse a cualquier interesado para la subsanación de deficiencias o la aportación de documentos y otros elementos de juicio necesarios, por el tiempo que medie entre la notificación del requerimiento y su efectivo cumplimiento por el destinatario, o, en su defecto, por el del plazo concedido, todo ello sin perjuicio de lo previsto en el artículo 68 de la presente Ley.

b) Cuando deba obtenerse un pronunciamiento previo y preceptivo de un órgano de la Unión Europea, por el tiempo que medie entre la petición, que habrá de comunicarse a los interesados, y la notificación del pronunciamiento a la Administración instructora, que también deberá serles comunicada.

c) Cuando exista un procedimiento no finalizado en el ámbito de la Unión Europea que condicione directamente el contenido de la resolución de que se trate, desde que se tenga constancia de su existencia, lo que deberá ser comunicado a los interesados, hasta que se resuelva, lo que también habrá de ser notificado.

d) Cuando se soliciten informes preceptivos a un órgano de la misma o distinta Administración, por el tiempo que medie entre la petición, que deberá comunicarse a los interesados, y la recepción del informe, que igualmente deberá ser comunicada a los mismos. Este plazo de suspensión no podrá exceder en ningún caso de tres meses. En caso de no recibirse el informe en el plazo indicado, proseguirá el procedimiento.

e) Cuando deban realizarse pruebas técnicas o análisis contradictorios o dirimentes propuestos por los interesados, durante el tiempo necesario para la incorporación de los resultados al expediente.

f) Cuando se inicien negociaciones con vistas a la conclusión de un pacto o convenio en los términos previstos en el artículo 86 de esta Ley, desde la declaración formal al respecto y hasta la conclusión sin efecto, en su caso, de las referidas negociaciones, que se constatará mediante declaración formulada por la Administración o los interesados.

g) Cuando para la resolución del procedimiento sea indispensable la obtención de un previo pronunciamiento por parte de un órgano jurisdiccional, desde el momento en que se solicita, lo que habrá de comunicarse a los interesados, hasta que la Administración tenga constancia del mismo, lo que también deberá serles comunicado.

2. El transcurso del plazo máximo legal para resolver un procedimiento y notificar la resolución se suspenderá en los siguientes casos:

a) Cuando una Administración Pública requiera a otra para que anule o revise un acto que entienda que es ilegal y que constituya la base para el que la primera haya de dictar en el ámbito de sus competencias, en el supuesto al que se refiere el apartado 5 del artículo 39 de esta Ley, desde que se realiza el requerimiento hasta que se atienda o, en su caso, se resuelva el recurso interpuesto ante la jurisdicción contencioso administrativa. Deberá ser comunicado a los interesados tanto la realización del requerimiento, como su cumplimiento o, en su caso, la resolución del correspondiente recurso contencioso-administrativo.

b) Cuando el órgano competente para resolver decida realizar alguna actuación complementaria de las previstas en el artículo 87, desde el momento en que se notifique a los interesados el acuerdo motivado del inicio de las actuaciones hasta que se produzca su terminación.

c) Cuando los interesados promuevan la recusación en cualquier momento de la tramitación de un procedimiento, desde que ésta se plantee hasta que sea resuelta por el superior jerárquico del recusado.

Artículo 23. *Ampliación del plazo máximo para resolver y notificar.*

1. Excepcionalmente, cuando se hayan agotado los medios personales y materiales disponibles a los que se refiere el apartado 5 del artículo 21, el órgano competente para resolver, a propuesta, en su caso, del órgano instructor o el superior jerárquico del órgano competente para resolver, podrá acordar de manera motivada la ampliación del plazo máximo de resolución y notificación, no pudiendo ser éste superior al establecido para la tramitación del procedimiento.

2. Contra el acuerdo que resuelva sobre la ampliación de plazos, que deberá ser notificado a los interesados, no cabrá recurso alguno.

Artículo 24. *Silencio administrativo en procedimientos iniciados a solicitud del interesado.*

1. En los procedimientos iniciados a solicitud del interesado, sin perjuicio de la resolución que la Administración debe dictar en la forma prevista en el apartado 3 de este artículo, el vencimiento del plazo máximo sin haberse notificado resolución expresa, legitima al interesado o interesados para entenderla estimada por silencio administrativo, excepto en los supuestos en los que una norma con rango de ley o una norma de Derecho de la Unión Europea o de Derecho internacional aplicable en España establezcan lo contrario. Cuando el procedimiento tenga por objeto el acceso a actividades o su ejercicio, la ley que disponga el carácter desestimatorio del silencio deberá fundarse en la concurrencia de razones imperiosas de interés general.

El silencio tendrá efecto desestimatorio en los procedimientos relativos al ejercicio del derecho de petición, a que se refiere el artículo 29 de la Constitución, aquellos cuya estimación tuviera como consecuencia que se transfirieran al solicitante o a terceros facultades relativas al dominio público o al servicio público, impliquen el ejercicio de actividades que puedan dañar el medio ambiente y en los procedimientos de responsabilidad patrimonial de las Administraciones Públicas.

El sentido del silencio también será desestimatorio en los procedimientos de impugnación de actos y disposiciones y en los de revisión de oficio iniciados a solicitud de los interesados. No obstante, cuando el recurso de alzada se haya interpuesto contra la desestimación por silencio administrativo de una solicitud por el transcurso del plazo, se entenderá estimado el mismo si, llegado el plazo de resolución, el órgano administrativo competente no dictase y notificase resolución expresa, siempre que no se refiera a las materias enumeradas en el párrafo anterior de este apartado.

2. La estimación por silencio administrativo tiene a todos los efectos la consideración de acto administrativo finalizador del procedimiento. La desestimación por silencio

administrativo tiene los solos efectos de permitir a los interesados la interposición del recurso administrativo o contencioso-administrativo que resulte procedente.

3. La obligación de dictar resolución expresa a que se refiere el apartado primero del artículo 21 se sujetará al siguiente régimen:

a) En los casos de estimación por silencio administrativo, la resolución expresa posterior a la producción del acto sólo podrá dictarse de ser confirmatoria del mismo.

b) En los casos de desestimación por silencio administrativo, la resolución expresa posterior al vencimiento del plazo se adoptará por la Administración sin vinculación alguna al sentido del silencio.

4. Los actos administrativos producidos por silencio administrativo se podrán hacer valer tanto ante la Administración como ante cualquier persona física o jurídica, pública o privada. Los mismos producen efectos desde el vencimiento del plazo máximo en el que debe dictarse y notificarse la resolución expresa sin que la misma se haya expedido, y su existencia puede ser acreditada por cualquier medio de prueba admitido en Derecho, incluido el certificado acreditativo del silencio producido. Este certificado se expedirá de oficio por el órgano competente para resolver en el plazo de quince días desde que expire el plazo máximo para resolver el procedimiento. Sin perjuicio de lo anterior, el interesado podrá pedirlo en cualquier momento, computándose el plazo indicado anteriormente desde el día siguiente a aquél en que la petición tuviese entrada en el registro electrónico de la Administración u Organismo competente para resolver.

Artículo 25. *Falta de resolución expresa en procedimientos iniciados de oficio.*

1. En los procedimientos iniciados de oficio, el vencimiento del plazo máximo establecido sin que se haya dictado y notificado resolución expresa no exime a la Administración del cumplimiento de la obligación legal de resolver, produciendo los siguientes efectos:

a) En el caso de procedimientos de los que pudiera derivarse el reconocimiento o, en su caso, la constitución de derechos u otras situaciones jurídicas favorables, los interesados que hubieren comparecido podrán entender desestimadas sus pretensiones por silencio administrativo.

b) En los procedimientos en que la Administración ejercite potestades sancionadoras o, en general, de intervención, susceptibles de producir efectos desfavorables o de gravamen, se producirá la caducidad. En estos casos, la resolución que declare la caducidad ordenará el archivo de las actuaciones, con los efectos previstos en el artículo 95.

2. En los supuestos en los que el procedimiento se hubiera paralizado por causa imputable al interesado, se interrumpirá el cómputo del plazo para resolver y notificar la resolución.

Artículo 26. *Emisión de documentos por las Administraciones Públicas.*

1. Se entiende por documentos públicos administrativos los válidamente emitidos por los órganos de las Administraciones Públicas. Las Administraciones Públicas emitirán los documentos administrativos por escrito, a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia.

2. Para ser considerados válidos, los documentos electrónicos administrativos deberán:

a) Contener información de cualquier naturaleza archivada en un soporte electrónico según un formato determinado susceptible de identificación y tratamiento diferenciado.

b) Disponer de los datos de identificación que permitan su individualización, sin perjuicio de su posible incorporación a un expediente electrónico.

c) Incorporar una referencia temporal del momento en que han sido emitidos.

d) Incorporar los metadatos mínimos exigidos.

e) Incorporar las firmas electrónicas que correspondan de acuerdo con lo previsto en la normativa aplicable.

Se considerarán válidos los documentos electrónicos, que cumpliendo estos requisitos, sean trasladados a un tercero a través de medios electrónicos.

3. No requerirán de firma electrónica, los documentos electrónicos emitidos por las Administraciones Públicas que se publiquen con carácter meramente informativo, así como aquellos que no formen parte de un expediente administrativo. En todo caso, será necesario identificar el origen de estos documentos.

Artículo 27. *Validez y eficacia de las copias realizadas por las Administraciones Públicas.*

1. Cada Administración Pública determinará los órganos que tengan atribuidas las competencias de expedición de copias auténticas de los documentos públicos administrativos o privados.

Las copias auténticas de documentos privados surten únicamente efectos administrativos. Las copias auténticas realizadas por una Administración Pública tendrán validez en las restantes Administraciones.

A estos efectos, la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales podrán realizar copias auténticas mediante funcionario habilitado o mediante actuación administrativa automatizada.

Se deberá mantener actualizado un registro, u otro sistema equivalente, donde constarán los funcionarios habilitados para la expedición de copias auténticas que deberán ser plenamente interoperables y estar interconectados con los de las restantes Administraciones Públicas, a los efectos de comprobar la validez de la citada habilitación. En este registro o sistema equivalente constarán, al menos, los funcionarios que presten servicios en las oficinas de asistencia en materia de registros.

2. Tendrán la consideración de copia auténtica de un documento público administrativo o privado las realizadas, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

Las copias auténticas tendrán la misma validez y eficacia que los documentos originales.

3. Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, así como a las siguientes reglas:

a) Las copias electrónicas de un documento electrónico original o de una copia electrónica auténtica, con o sin cambio de formato, deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

b) Las copias electrónicas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización, requerirán que el documento haya sido digitalizado y deberán incluir los metadatos que acrediten su condición de copia y que se visualicen al consultar el documento.

Se entiende por digitalización, el proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en un fichero electrónico que contiene la imagen codificada, fiel e íntegra del documento.

c) Las copias en soporte papel de documentos electrónicos requerirán que en las mismas figure la condición de copia y contendrán un código generado electrónicamente u otro sistema de verificación, que permitirá contrastar la autenticidad de la copia mediante el acceso a los archivos electrónicos del órgano u Organismo público emisor.

d) Las copias en soporte papel de documentos originales emitidos en dicho soporte se proporcionarán mediante una copia auténtica en papel del documento electrónico que se encuentre en poder de la Administración o bien mediante una puesta de manifiesto electrónica conteniendo copia auténtica del documento original.

A estos efectos, las Administraciones harán públicos, a través de la sede electrónica correspondiente, los códigos seguros de verificación u otro sistema de verificación utilizado.

4. Los interesados podrán solicitar, en cualquier momento, la expedición de copias auténticas de los documentos públicos administrativos que hayan sido válidamente emitidos por las Administraciones Públicas. La solicitud se dirigirá al órgano que emitió el documento original, debiendo expedirse, salvo las excepciones derivadas de la aplicación de la Ley 19/2013, de 9 de diciembre, en el plazo de quince días a contar desde la recepción de la solicitud en el registro electrónico de la Administración u Organismo competente.

Asimismo, las Administraciones Públicas estarán obligadas a expedir copias auténticas electrónicas de cualquier documento en papel que presenten los interesados y que se vaya a incorporar a un expediente administrativo.

5. Cuando las Administraciones Públicas expidan copias auténticas electrónicas, deberá quedar expresamente así indicado en el documento de la copia.

6. La expedición de copias auténticas de documentos públicos notariales, registrales y judiciales, así como de los diarios oficiales, se regirá por su legislación específica.

Artículo 28. *Documentos aportados por los interesados al procedimiento administrativo.*

1. Los interesados deberán aportar al procedimiento administrativo los datos y documentos exigidos por las Administraciones Públicas de acuerdo con lo dispuesto en la normativa aplicable. Asimismo, los interesados podrán aportar cualquier otro documento que estimen conveniente.

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.

4. Cuando con carácter excepcional, y de acuerdo con lo previsto en esta Ley, la Administración solicitara al interesado la presentación de un documento original y éste estuviera en formato papel, el interesado deberá obtener una copia auténtica, según los requisitos establecidos en el artículo 27, con carácter previo a su presentación electrónica. La copia electrónica resultante reflejará expresamente esta circunstancia.

5. Excepcionalmente, cuando la relevancia del documento en el procedimiento lo exija o existan dudas derivadas de la calidad de la copia, las Administraciones podrán solicitar de manera motivada el cotejo de las copias aportadas por el interesado, para lo que podrán requerir la exhibición del documento o de la información original.

6. Las copias que aporten los interesados al procedimiento administrativo tendrán eficacia, exclusivamente en el ámbito de la actividad de las Administraciones Públicas.

7. Los interesados se responsabilizarán de la veracidad de los documentos que presenten.

CAPÍTULO II

Términos y plazos

Artículo 29. *Obligatoriedad de términos y plazos.*

Los términos y plazos establecidos en ésta u otras leyes obligan a las autoridades y personal al servicio de las Administraciones Públicas competentes para la tramitación de los asuntos, así como a los interesados en los mismos.

Artículo 30. *Cómputo de plazos.*

1. Salvo que por Ley o en el Derecho de la Unión Europea se disponga otro cómputo, cuando los plazos se señalen por horas, se entiende que éstas son hábiles. Son hábiles todas las horas del día que formen parte de un día hábil.

Los plazos expresados por horas se contarán de hora en hora y de minuto en minuto desde la hora y minuto en que tenga lugar la notificación o publicación del acto de que se trate y no podrán tener una duración superior a veinticuatro horas, en cuyo caso se expresarán en días.

2. Siempre que por Ley o en el Derecho de la Unión Europea no se exprese otro cómputo, cuando los plazos se señalen por días, se entiende que éstos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

Cuando los plazos se hayan señalado por días naturales por declararlo así una ley o por el Derecho de la Unión Europea, se hará constar esta circunstancia en las correspondientes notificaciones.

3. Los plazos expresados en días se contarán a partir del día siguiente a aquel en que tenga lugar la notificación o publicación del acto de que se trate, o desde el siguiente a aquel en que se produzca la estimación o la desestimación por silencio administrativo.

4. Si el plazo se fija en meses o años, éstos se computarán a partir del día siguiente a aquel en que tenga lugar la notificación o publicación del acto de que se trate, o desde el siguiente a aquel en que se produzca la estimación o desestimación por silencio administrativo.

El plazo concluirá el mismo día en que se produjo la notificación, publicación o silencio administrativo en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

5. Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

6. Cuando un día fuese hábil en el municipio o Comunidad Autónoma en que residiese el interesado, e inhábil en la sede del órgano administrativo, o a la inversa, se considerará inhábil en todo caso.

7. La Administración General del Estado y las Administraciones de las Comunidades Autónomas, con sujeción al calendario laboral oficial, fijarán, en su respectivo ámbito, el calendario de días inhábiles a efectos de cómputos de plazos. El calendario aprobado por las Comunidades Autónomas comprenderá los días inhábiles de las Entidades Locales correspondientes a su ámbito territorial, a las que será de aplicación.

Dicho calendario deberá publicarse antes del comienzo de cada año en el diario oficial que corresponda, así como en otros medios de difusión que garanticen su conocimiento generalizado.

8. La declaración de un día como hábil o inhábil a efectos de cómputo de plazos no determina por sí sola el funcionamiento de los centros de trabajo de las Administraciones Públicas, la organización del tiempo de trabajo o el régimen de jornada y horarios de las mismas.

Artículo 31. *Cómputo de plazos en los registros.*

1. Cada Administración Pública publicará los días y el horario en el que deban permanecer abiertas las oficinas que prestarán asistencia para la presentación electrónica de documentos, garantizando el derecho de los interesados a ser asistidos en el uso de medios electrónicos.

2. El registro electrónico de cada Administración u Organismo se regirá a efectos de cómputo de los plazos, por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar de modo accesible y visible.

El funcionamiento del registro electrónico se regirá por las siguientes reglas:

a) Permitirá la presentación de documentos todos los días del año durante las veinticuatro horas.

b) A los efectos del cómputo de plazo fijado en días hábiles, y en lo que se refiere al cumplimiento de plazos por los interesados, la presentación en un día inhábil se entenderá realizada en la primera hora del primer día hábil siguiente salvo que una norma permita expresamente la recepción en día inhábil.

Los documentos se considerarán presentados por el orden de hora efectiva en el que lo fueron en el día inhábil. Los documentos presentados en el día inhábil se reputarán anteriores, según el mismo orden, a los que lo fueran el primer día hábil posterior.

c) El inicio del cómputo de los plazos que hayan de cumplir las Administraciones Públicas vendrá determinado por la fecha y hora de presentación en el registro electrónico de cada Administración u Organismo. En todo caso, la fecha y hora efectiva de inicio del cómputo de plazos deberá ser comunicada a quien presentó el documento.

3. La sede electrónica del registro de cada Administración Pública u Organismo, determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquélla y al calendario previsto en el artículo 30.7, los días que se considerarán inhábiles a los efectos previstos en este artículo. Este será el único calendario de días inhábiles que se aplicará a efectos del cómputo de plazos en los registros electrónicos, sin que resulte de aplicación a los mismos lo dispuesto en el artículo 30.6.

Artículo 32. *Ampliación.*

1. La Administración, salvo precepto en contrario, podrá conceder de oficio o a petición de los interesados, una ampliación de los plazos establecidos, que no exceda de la mitad de los mismos, si las circunstancias lo aconsejan y con ello no se perjudican derechos de tercero. El acuerdo de ampliación deberá ser notificado a los interesados.

2. La ampliación de los plazos por el tiempo máximo permitido se aplicará en todo caso a los procedimientos tramitados por las misiones diplomáticas y oficinas consulares, así como a aquellos que, sustanciándose en el interior, exijan cumplimentar algún trámite en el extranjero o en los que intervengan interesados residentes fuera de España.

3. Tanto la petición de los interesados como la decisión sobre la ampliación deberán producirse, en todo caso, antes del vencimiento del plazo de que se trate. En ningún caso podrá ser objeto de ampliación un plazo ya vencido. Los acuerdos sobre ampliación de plazos o sobre su denegación no serán susceptibles de recurso, sin perjuicio del procedente contra la resolución que ponga fin al procedimiento.

4. Cuando una incidencia técnica haya imposibilitado el funcionamiento ordinario del sistema o aplicación que corresponda, y hasta que se solucione el problema, la Administración podrá determinar una ampliación de los plazos no vencidos, debiendo publicar en la sede electrónica tanto la incidencia técnica acontecida como la ampliación concreta del plazo no vencido.

5. Cuando como consecuencia de un ciberincidente se hayan visto gravemente afectados los servicios y sistemas utilizados para la tramitación de los procedimientos y el ejercicio de los derechos de los interesados que prevé la normativa vigente, la Administración podrá acordar la ampliación general de plazos de los procedimientos administrativos.

Artículo 33. *Tramitación de urgencia.*

1. Cuando razones de interés público lo aconsejen, se podrá acordar, de oficio o a petición del interesado, la aplicación al procedimiento de la tramitación de urgencia, por la cual se reducirán a la mitad los plazos establecidos para el procedimiento ordinario, salvo los relativos a la presentación de solicitudes y recursos.

2. No cabrá recurso alguno contra el acuerdo que declare la aplicación de la tramitación de urgencia al procedimiento, sin perjuicio del procedente contra la resolución que ponga fin al procedimiento.

TÍTULO III

De los actos administrativos

CAPÍTULO I

Requisitos de los actos administrativos

Artículo 34. *Producción y contenido.*

1. Los actos administrativos que dicten las Administraciones Públicas, bien de oficio o a instancia del interesado, se producirán por el órgano competente ajustándose a los requisitos y al procedimiento establecido.

2. El contenido de los actos se ajustará a lo dispuesto por el ordenamiento jurídico y será determinado y adecuado a los fines de aquéllos.

Artículo 35. *Motivación.*

1. Serán motivados, con sucinta referencia de hechos y fundamentos de derecho:

a) Los actos que limiten derechos subjetivos o intereses legítimos.

b) Los actos que resuelvan procedimientos de revisión de oficio de disposiciones o actos administrativos, recursos administrativos y procedimientos de arbitraje y los que declaren su inadmisión.

c) Los actos que se separen del criterio seguido en actuaciones precedentes o del dictamen de órganos consultivos.

d) Los acuerdos de suspensión de actos, cualquiera que sea el motivo de ésta, así como la adopción de medidas provisionales previstas en el artículo 56.

e) Los acuerdos de aplicación de la tramitación de urgencia, de ampliación de plazos y de realización de actuaciones complementarias.

f) Los actos que rechacen pruebas propuestas por los interesados.

g) Los actos que acuerden la terminación del procedimiento por la imposibilidad material de continuarlo por causas sobrevenidas, así como los que acuerden el desistimiento por la Administración en procedimientos iniciados de oficio.

h) Las propuestas de resolución en los procedimientos de carácter sancionador, así como los actos que resuelvan procedimientos de carácter sancionador o de responsabilidad patrimonial.

i) Los actos que se dicten en el ejercicio de potestades discrecionales, así como los que deban serlo en virtud de disposición legal o reglamentaria expresa.

2. La motivación de los actos que pongan fin a los procedimientos selectivos y de concurrencia competitiva se realizará de conformidad con lo que dispongan las normas que regulen sus convocatorias, debiendo, en todo caso, quedar acreditados en el procedimiento los fundamentos de la resolución que se adopte.

Artículo 36. *Forma.*

1. Los actos administrativos se producirán por escrito a través de medios electrónicos, a menos que su naturaleza exija otra forma más adecuada de expresión y constancia.

2. En los casos en que los órganos administrativos ejerzan su competencia de forma verbal, la constancia escrita del acto, cuando sea necesaria, se efectuará y firmará por el titular del órgano inferior o funcionario que la reciba oralmente, expresando en la comunicación del mismo la autoridad de la que procede. Si se tratara de resoluciones, el titular de la competencia deberá autorizar una relación de las que haya dictado de forma verbal, con expresión de su contenido.

3. Cuando deba dictarse una serie de actos administrativos de la misma naturaleza, tales como nombramientos, concesiones o licencias, podrán refundirse en un único acto, acordado por el órgano competente, que especificará las personas u otras circunstancias que individualicen los efectos del acto para cada interesado.

CAPÍTULO II

Eficacia de los actos

Artículo 37. *Inderogabilidad singular.*

1. Las resoluciones administrativas de carácter particular no podrán vulnerar lo establecido en una disposición de carácter general, aunque aquéllas procedan de un órgano de igual o superior jerarquía al que dictó la disposición general.
2. Son nulas las resoluciones administrativas que vulneren lo establecido en una disposición reglamentaria, así como aquellas que incurran en alguna de las causas recogidas en el artículo 47.

Artículo 38. *Ejecutividad.*

Los actos de las Administraciones Públicas sujetos al Derecho Administrativo serán ejecutivos con arreglo a lo dispuesto en esta Ley.

Artículo 39. *Efectos.*

1. Los actos de las Administraciones Públicas sujetos al Derecho Administrativo se presumirán válidos y producirán efectos desde la fecha en que se dicten, salvo que en ellos se disponga otra cosa.
2. La eficacia quedará demorada cuando así lo exija el contenido del acto o esté supeditada a su notificación, publicación o aprobación superior.
3. Excepcionalmente, podrá otorgarse eficacia retroactiva a los actos cuando se dicten en sustitución de actos anulados, así como cuando produzcan efectos favorables al interesado, siempre que los supuestos de hecho necesarios existieran ya en la fecha a que se retrotraiga la eficacia del acto y ésta no lesione derechos o intereses legítimos de otras personas.
4. Las normas y actos dictados por los órganos de las Administraciones Públicas en el ejercicio de su propia competencia deberán ser observadas por el resto de los órganos administrativos, aunque no dependan jerárquicamente entre sí o pertenezcan a otra Administración.
5. Cuando una Administración Pública tenga que dictar, en el ámbito de sus competencias, un acto que necesariamente tenga por base otro dictado por una Administración Pública distinta y aquélla entienda que es ilegal, podrá requerir a ésta previamente para que anule o revise el acto de acuerdo con lo dispuesto en el artículo 44 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso- Administrativa, y, de rechazar el requerimiento, podrá interponer recurso contencioso-administrativo. En estos casos, quedará suspendido el procedimiento para dictar resolución.

Artículo 40. *Notificación.*

1. El órgano que dicte las resoluciones y actos administrativos los notificará a los interesados cuyos derechos e intereses sean afectados por aquéllos, en los términos previstos en los artículos siguientes.
2. Toda notificación deberá ser cursada dentro del plazo de diez días a partir de la fecha en que el acto haya sido dictado, y deberá contener el texto íntegro de la resolución, con indicación de si pone fin o no a la vía administrativa, la expresión de los recursos que procedan, en su caso, en vía administrativa y judicial, el órgano ante el que hubieran de presentarse y el plazo para interponerlos, sin perjuicio de que los interesados puedan ejercitar, en su caso, cualquier otro que estimen procedente.
3. Las notificaciones que, conteniendo el texto íntegro del acto, omitiesen alguno de los demás requisitos previstos en el apartado anterior, surtirán efecto a partir de la fecha en que

el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación, o interponga cualquier recurso que proceda.

4. Sin perjuicio de lo establecido en el apartado anterior, y a los solos efectos de entender cumplida la obligación de notificar dentro del plazo máximo de duración de los procedimientos, será suficiente la notificación que contenga, cuando menos, el texto íntegro de la resolución, así como el intento de notificación debidamente acreditado.

5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la protección de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado.

Artículo 41. *Condiciones generales para la práctica de las notificaciones.*

1. Las notificaciones se practicarán preferentemente por medios electrónicos y, en todo caso, cuando el interesado resulte obligado a recibirlas por esta vía.

No obstante lo anterior, las Administraciones podrán practicar las notificaciones por medios no electrónicos en los siguientes supuestos:

a) Cuando la notificación se realice con ocasión de la comparecencia espontánea del interesado o su representante en las oficinas de asistencia en materia de registro y solicite la comunicación o notificación personal en ese momento.

b) Cuando para asegurar la eficacia de la actuación administrativa resulte necesario practicar la notificación por entrega directa de un empleado público de la Administración notificante.

Con independencia del medio utilizado, las notificaciones serán válidas siempre que permitan tener constancia de su envío o puesta a disposición, de la recepción o acceso por el interesado o su representante, de sus fechas y horas, del contenido íntegro, y de la identidad fidedigna del remitente y destinatario de la misma. La acreditación de la notificación efectuada se incorporará al expediente.

Los interesados que no estén obligados a recibir notificaciones electrónicas, podrán decidir y comunicar en cualquier momento a la Administración Pública, mediante los modelos normalizados que se establezcan al efecto, que las notificaciones sucesivas se practiquen o dejen de practicarse por medios electrónicos.

Reglamentariamente, las Administraciones podrán establecer la obligación de practicar electrónicamente las notificaciones para determinados procedimientos y para ciertos colectivos de personas físicas que por razón de su capacidad económica, técnica, dedicación profesional u otros motivos quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

Adicionalmente, el interesado podrá identificar un dispositivo electrónico y/o una dirección de correo electrónico que servirán para el envío de los avisos regulados en este artículo, pero no para la práctica de notificaciones.

2. En ningún caso se efectuarán por medios electrónicos las siguientes notificaciones:

a) Aquellas en las que el acto a notificar vaya acompañado de elementos que no sean susceptibles de conversión en formato electrónico.

b) Las que contengan medios de pago a favor de los obligados, tales como cheques.

3. En los procedimientos iniciados a solicitud del interesado, la notificación se practicará por el medio señalado al efecto por aquel. Esta notificación será electrónica en los casos en los que exista obligación de relacionarse de esta forma con la Administración.

Cuando no fuera posible realizar la notificación de acuerdo con lo señalado en la solicitud, se practicará en cualquier lugar adecuado a tal fin, y por cualquier medio que permita tener constancia de la recepción por el interesado o su representante, así como de la fecha, la identidad y el contenido del acto notificado.

4. En los procedimientos iniciados de oficio, a los solos efectos de su iniciación, las Administraciones Públicas podrán recabar, mediante consulta a las bases de datos del Instituto Nacional de Estadística, los datos sobre el domicilio del interesado recogidos en el Padrón Municipal, remitidos por las Entidades Locales en aplicación de lo previsto en la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

5. Cuando el interesado o su representante rechace la notificación de una actuación administrativa, se hará constar en el expediente, especificándose las circunstancias del intento de notificación y el medio, dando por efectuado el trámite y siguiéndose el procedimiento.

6. Con independencia de que la notificación se realice en papel o por medios electrónicos, las Administraciones Públicas enviarán un aviso al dispositivo electrónico y/o a la dirección de correo electrónico del interesado que éste haya comunicado, informándole de la puesta a disposición de una notificación en la sede electrónica de la Administración u Organismo correspondiente o en la dirección electrónica habilitada única. La falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

7. Cuando el interesado fuera notificado por distintos cauces, se tomará como fecha de notificación la de aquélla que se hubiera producido en primer lugar.

Artículo 42. *Práctica de las notificaciones en papel.*

1. Todas las notificaciones que se practiquen en papel deberán ser puestas a disposición del interesado en la sede electrónica de la Administración u Organismo actuante para que pueda acceder al contenido de las mismas de forma voluntaria.

2. Cuando la notificación se practique en el domicilio del interesado, de no hallarse presente éste en el momento de entregarse la notificación, podrá hacerse cargo de la misma cualquier persona mayor de catorce años que se encuentre en el domicilio y haga constar su identidad. Si nadie se hiciera cargo de la notificación, se hará constar esta circunstancia en el expediente, junto con el día y la hora en que se intentó la notificación, intento que se repetirá por una sola vez y en una hora distinta dentro de los tres días siguientes. En caso de que el primer intento de notificación se haya realizado antes de las quince horas, el segundo intento deberá realizarse después de las quince horas y viceversa, dejando en todo caso al menos un margen de diferencia de tres horas entre ambos intentos de notificación. Si el segundo intento también resultara infructuoso, se procederá en la forma prevista en el artículo 44.

3. Cuando el interesado accediera al contenido de la notificación en sede electrónica, se le ofrecerá la posibilidad de que el resto de notificaciones se puedan realizar a través de medios electrónicos.

Artículo 43. *Práctica de las notificaciones a través de medios electrónicos.*

1. Las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica de la Administración u Organismo actuante, a través de la dirección electrónica habilitada única o mediante ambos sistemas, según disponga cada Administración u Organismo.

A los efectos previstos en este artículo, se entiende por comparecencia en la sede electrónica, el acceso por el interesado o su representante debidamente identificado al contenido de la notificación.

2. Las notificaciones por medios electrónicos se entenderán practicadas en el momento en que se produzca el acceso a su contenido.

Cuando la notificación por medios electrónicos sea de carácter obligatorio, o haya sido expresamente elegida por el interesado, se entenderá rechazada cuando hayan transcurrido diez días naturales desde la puesta a disposición de la notificación sin que se acceda a su contenido.

3. Se entenderá cumplida la obligación a la que se refiere el artículo 40.4 con la puesta a disposición de la notificación en la sede electrónica de la Administración u Organismo actuante o en la dirección electrónica habilitada única.

4. Los interesados podrán acceder a las notificaciones desde el Punto de Acceso General electrónico de la Administración, que funcionará como un portal de acceso.

Artículo 44. *Notificación infructuosa.*

Cuando los interesados en un procedimiento sean desconocidos, se ignore el lugar de la notificación o bien, intentada ésta, no se hubiese podido practicar, la notificación se hará por medio de un anuncio publicado en el «Boletín Oficial del Estado».

Asimismo, previamente y con carácter facultativo, las Administraciones podrán publicar un anuncio en el boletín oficial de la Comunidad Autónoma o de la Provincia, en el tablón de edictos del Ayuntamiento del último domicilio del interesado o del Consulado o Sección Consular de la Embajada correspondiente.

Las Administraciones Públicas podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión, que no excluirán la obligación de publicar el correspondiente anuncio en el «Boletín Oficial del Estado».

Artículo 45. *Publicación.*

1. Los actos administrativos serán objeto de publicación cuando así lo establezcan las normas reguladoras de cada procedimiento o cuando lo aconsejen razones de interés público apreciadas por el órgano competente.

En todo caso, los actos administrativos serán objeto de publicación, surtiendo ésta los efectos de la notificación, en los siguientes casos:

a) Cuando el acto tenga por destinatario a una pluralidad indeterminada de personas o cuando la Administración estime que la notificación efectuada a un solo interesado es insuficiente para garantizar la notificación a todos, siendo, en este último caso, adicional a la individualmente realizada.

b) Cuando se trate de actos integrantes de un procedimiento selectivo o de concurrencia competitiva de cualquier tipo. En este caso, la convocatoria del procedimiento deberá indicar el medio donde se efectuarán las sucesivas publicaciones, careciendo de validez las que se lleven a cabo en lugares distintos.

2. La publicación de un acto deberá contener los mismos elementos que el artículo 40.2 exige respecto de las notificaciones. Será también aplicable a la publicación lo establecido en el apartado 3 del mismo artículo.

En los supuestos de publicaciones de actos que contengan elementos comunes, podrán publicarse de forma conjunta los aspectos coincidentes, especificándose solamente los aspectos individuales de cada acto.

3. La publicación de los actos se realizará en el diario oficial que corresponda, según cual sea la Administración de la que proceda el acto a notificar.

4. Sin perjuicio de lo dispuesto en el artículo 44, la publicación de actos y comunicaciones que, por disposición legal o reglamentaria deba practicarse en tablón de anuncios o edictos, se entenderá cumplida por su publicación en el Diario oficial correspondiente.

Artículo 46. *Indicación de notificaciones y publicaciones.*

Si el órgano competente apreciase que la notificación por medio de anuncios o la publicación de un acto lesiona derechos o intereses legítimos, se limitará a publicar en el Diario oficial que corresponda una somera indicación del contenido del acto y del lugar donde los interesados podrán comparecer, en el plazo que se establezca, para conocimiento del contenido íntegro del mencionado acto y constancia de tal conocimiento.

Adicionalmente y de manera facultativa, las Administraciones podrán establecer otras formas de notificación complementarias a través de los restantes medios de difusión que no excluirán la obligación de publicar en el correspondiente Diario oficial.

CAPÍTULO III

Nulidad y anulabilidad

Artículo 47. *Nulidad de pleno derecho.*

1. Los actos de las Administraciones Públicas son nulos de pleno derecho en los casos siguientes:

a) Los que lesionen los derechos y libertades susceptibles de amparo constitucional.

b) Los dictados por órgano manifiestamente incompetente por razón de la materia o del territorio.

c) Los que tengan un contenido imposible.

d) Los que sean constitutivos de infracción penal o se dicten como consecuencia de ésta.

e) Los dictados prescindiendo total y absolutamente del procedimiento legalmente establecido o de las normas que contienen las reglas esenciales para la formación de la voluntad de los órganos colegiados.

f) Los actos expresos o presuntos contrarios al ordenamiento jurídico por los que se adquieren facultades o derechos cuando se carezca de los requisitos esenciales para su adquisición.

g) Cualquier otro que se establezca expresamente en una disposición con rango de Ley.

2. También serán nulas de pleno derecho las disposiciones administrativas que vulneren la Constitución, las leyes u otras disposiciones administrativas de rango superior, las que regulen materias reservadas a la Ley, y las que establezcan la retroactividad de disposiciones sancionadoras no favorables o restrictivas de derechos individuales.

Artículo 48. *Anulabilidad.*

1. Son anulables los actos de la Administración que incurran en cualquier infracción del ordenamiento jurídico, incluso la desviación de poder.

2. No obstante, el defecto de forma sólo determinará la anulabilidad cuando el acto carezca de los requisitos formales indispensables para alcanzar su fin o dé lugar a la indefensión de los interesados.

3. La realización de actuaciones administrativas fuera del tiempo establecido para ellas sólo implicará la anulabilidad del acto cuando así lo imponga la naturaleza del término o plazo.

Artículo 49. *Límites a la extensión de la nulidad o anulabilidad de los actos.*

1. La nulidad o anulabilidad de un acto no implicará la de los sucesivos en el procedimiento que sean independientes del primero.

2. La nulidad o anulabilidad en parte del acto administrativo no implicará la de las partes del mismo independientes de aquélla, salvo que la parte viciada sea de tal importancia que sin ella el acto administrativo no hubiera sido dictado.

Artículo 50. *Conversión de actos viciados.*

Los actos nulos o anulables que, sin embargo, contengan los elementos constitutivos de otro distinto producirán los efectos de éste.

Artículo 51. *Conservación de actos y trámites.*

El órgano que declare la nulidad o anule las actuaciones dispondrá siempre la conservación de aquellos actos y trámites cuyo contenido se hubiera mantenido igual de no haberse cometido la infracción.

Artículo 52. *Convalidación.*

1. La Administración podrá convalidar los actos anulables, subsanando los vicios de que adolezcan.

2. El acto de convalidación producirá efecto desde su fecha, salvo lo dispuesto en el artículo 39.3 para la retroactividad de los actos administrativos.

3. Si el vicio consistiera en incompetencia no determinante de nulidad, la convalidación podrá realizarse por el órgano competente cuando sea superior jerárquico del que dictó el acto viciado.

4. Si el vicio consistiese en la falta de alguna autorización, podrá ser convalidado el acto mediante el otorgamiento de la misma por el órgano competente.

TÍTULO IV

De las disposiciones sobre el procedimiento administrativo común

CAPÍTULO I

Garantías del procedimiento

Artículo 53. *Derechos del interesado en el procedimiento administrativo.*

1. Además del resto de derechos previstos en esta Ley, los interesados en un procedimiento administrativo, tienen los siguientes derechos:

a) A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados; el sentido del silencio administrativo que corresponda, en caso de que la Administración no dicte ni notifique resolución expresa en plazo; el órgano competente para su instrucción, en su caso, y resolución; y los actos de trámite dictados. Asimismo, también tendrán derecho a acceder y a obtener copia de los documentos contenidos en los citados procedimientos.

Quienes se relacionen con las Administraciones Públicas a través de medios electrónicos, tendrán derecho a consultar la información a la que se refiere el párrafo anterior, en el Punto de Acceso General electrónico de la Administración que funcionará como un portal de acceso. Se entenderá cumplida la obligación de la Administración de facilitar copias de los documentos contenidos en los procedimientos mediante la puesta a disposición de las mismas en el Punto de Acceso General electrónico de la Administración competente o en las sedes electrónicas que correspondan.

b) A identificar a las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos.

c) A no presentar documentos originales salvo que, de manera excepcional, la normativa reguladora aplicable establezca lo contrario. En caso de que, excepcionalmente, deban presentar un documento original, tendrán derecho a obtener una copia autenticada de éste.

d) A no presentar datos y documentos no exigidos por las normas aplicables al procedimiento de que se trate, que ya se encuentren en poder de las Administraciones Públicas o que hayan sido elaborados por éstas.

e) A formular alegaciones, utilizar los medios de defensa admitidos por el Ordenamiento Jurídico, y a aportar documentos en cualquier fase del procedimiento anterior al trámite de audiencia, que deberán ser tenidos en cuenta por el órgano competente al redactar la propuesta de resolución.

f) A obtener información y orientación acerca de los requisitos jurídicos o técnicos que las disposiciones vigentes impongan a los proyectos, actuaciones o solicitudes que se propongan realizar.

g) A actuar asistidos de asesor cuando lo consideren conveniente en defensa de sus intereses.

h) A cumplir las obligaciones de pago a través de los medios electrónicos previstos en el artículo 98.2.

i) Cualesquiera otros que les reconozcan la Constitución y las leyes.

2. Además de los derechos previstos en el apartado anterior, en el caso de procedimientos administrativos de naturaleza sancionadora, los presuntos responsables tendrán los siguientes derechos:

a) A ser notificado de los hechos que se le imputen, de las infracciones que tales hechos puedan constituir y de las sanciones que, en su caso, se les pudieran imponer, así como de la identidad del instructor, de la autoridad competente para imponer la sanción y de la norma que atribuya tal competencia.

b) A la presunción de no existencia de responsabilidad administrativa mientras no se demuestre lo contrario.

CAPÍTULO II

Iniciación del procedimiento

Sección 1.ª Disposiciones generales

Artículo 54. *Clases de iniciación.*

Los procedimientos podrán iniciarse de oficio o a solicitud del interesado.

Artículo 55. *Información y actuaciones previas.*

1. Con anterioridad al inicio del procedimiento, el órgano competente podrá abrir un período de información o actuaciones previas con el fin de conocer las circunstancias del caso concreto y la conveniencia o no de iniciar el procedimiento.

2. En el caso de procedimientos de naturaleza sancionadora las actuaciones previas se orientarán a determinar, con la mayor precisión posible, los hechos susceptibles de motivar la incoación del procedimiento, la identificación de la persona o personas que pudieran resultar responsables y las circunstancias relevantes que concurran en unos y otros.

Las actuaciones previas serán realizadas por los órganos que tengan atribuidas funciones de investigación, averiguación e inspección en la materia y, en defecto de éstos, por la persona u órgano administrativo que se determine por el órgano competente para la iniciación o resolución del procedimiento.

Artículo 56. *Medidas provisionales.*

1. Iniciado el procedimiento, el órgano administrativo competente para resolver, podrá adoptar, de oficio o a instancia de parte y de forma motivada, las medidas provisionales que estime oportunas para asegurar la eficacia de la resolución que pudiera recaer, si existiesen elementos de juicio suficientes para ello, de acuerdo con los principios de proporcionalidad, efectividad y menor onerosidad.

2. Antes de la iniciación del procedimiento administrativo, el órgano competente para iniciar o instruir el procedimiento, de oficio o a instancia de parte, en los casos de urgencia inaplazable y para la protección provisional de los intereses implicados, podrá adoptar de forma motivada las medidas provisionales que resulten necesarias y proporcionadas. Las medidas provisionales deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los quince días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

3. De acuerdo con lo previsto en los dos apartados anteriores, podrán acordarse las siguientes medidas provisionales, en los términos previstos en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil:

a) Suspensión temporal de actividades.

b) Prestación de fianzas.

c) Retirada o intervención de bienes productivos o suspensión temporal de servicios por razones de sanidad, higiene o seguridad, el cierre temporal del establecimiento por estas u otras causas previstas en la normativa reguladora aplicable.

d) Embargo preventivo de bienes, rentas y cosas fungibles computables en metálico por aplicación de precios ciertos.

e) El depósito, retención o inmovilización de cosa mueble.

f) La intervención y depósito de ingresos obtenidos mediante una actividad que se considere ilícita y cuya prohibición o cesación se pretenda.

g) Consignación o constitución de depósito de las cantidades que se reclamen.

h) La retención de ingresos a cuenta que deban abonar las Administraciones Públicas.

i) Aquellas otras medidas que, para la protección de los derechos de los interesados, prevean expresamente las leyes, o que se estimen necesarias para asegurar la efectividad de la resolución.

4. No se podrán adoptar medidas provisionales que puedan causar perjuicio de difícil o imposible reparación a los interesados o que impliquen violación de derechos amparados por las leyes.

5. Las medidas provisionales podrán ser alzadas o modificadas durante la tramitación del procedimiento, de oficio o a instancia de parte, en virtud de circunstancias sobrevenidas o que no pudieron ser tenidas en cuenta en el momento de su adopción.

En todo caso, se extinguirán cuando surta efectos la resolución administrativa que ponga fin al procedimiento correspondiente.

Artículo 57. *Acumulación.*

El órgano administrativo que inicie o tramite un procedimiento, cualquiera que haya sido la forma de su iniciación, podrá disponer, de oficio o a instancia de parte, su acumulación a otros con los que guarde identidad sustancial o íntima conexión, siempre que sea el mismo órgano quien deba tramitar y resolver el procedimiento.

Contra el acuerdo de acumulación no procederá recurso alguno.

Sección 2.ª Iniciación del procedimiento de oficio por la administración

Artículo 58. *Iniciación de oficio.*

Los procedimientos se iniciarán de oficio por acuerdo del órgano competente, bien por propia iniciativa o como consecuencia de orden superior, a petición razonada de otros órganos o por denuncia.

Artículo 59. *Inicio del procedimiento a propia iniciativa.*

Se entiende por propia iniciativa, la actuación derivada del conocimiento directo o indirecto de las circunstancias, conductas o hechos objeto del procedimiento por el órgano que tiene atribuida la competencia de iniciación.

Artículo 60. *Inicio del procedimiento como consecuencia de orden superior.*

1. Se entiende por orden superior, la emitida por un órgano administrativo superior jerárquico del competente para la iniciación del procedimiento.

2. En los procedimientos de naturaleza sancionadora, la orden expresará, en la medida de lo posible, la persona o personas presuntamente responsables; las conductas o hechos que pudieran constituir infracción administrativa y su tipificación; así como el lugar, la fecha, fechas o período de tiempo continuado en que los hechos se produjeron.

Artículo 61. *Inicio del procedimiento por petición razonada de otros órganos.*

1. Se entiende por petición razonada, la propuesta de iniciación del procedimiento formulada por cualquier órgano administrativo que no tiene competencia para iniciar el mismo y que ha tenido conocimiento de las circunstancias, conductas o hechos objeto del procedimiento, bien ocasionalmente o bien por tener atribuidas funciones de inspección, averiguación o investigación.

2. La petición no vincula al órgano competente para iniciar el procedimiento, si bien deberá comunicar al órgano que la hubiera formulado los motivos por los que, en su caso, no procede la iniciación.

3. En los procedimientos de naturaleza sancionadora, las peticiones deberán especificar, en la medida de lo posible, la persona o personas presuntamente responsables; las conductas o hechos que pudieran constituir infracción administrativa y su tipificación; así como el lugar, la fecha, fechas o período de tiempo continuado en que los hechos se produjeron.

4. En los procedimientos de responsabilidad patrimonial, la petición deberá individualizar la lesión producida en una persona o grupo de personas, su relación de causalidad con el funcionamiento del servicio público, su evaluación económica si fuera posible, y el momento en que la lesión efectivamente se produjo.

Artículo 62. *Inicio del procedimiento por denuncia.*

1. Se entiende por denuncia, el acto por el que cualquier persona, en cumplimiento o no de una obligación legal, pone en conocimiento de un órgano administrativo la existencia de un determinado hecho que pudiera justificar la iniciación de oficio de un procedimiento administrativo.

2. Las denuncias deberán expresar la identidad de la persona o personas que las presentan y el relato de los hechos que se ponen en conocimiento de la Administración. Cuando dichos hechos pudieran constituir una infracción administrativa, recogerán la fecha de su comisión y, cuando sea posible, la identificación de los presuntos responsables.

3. Cuando la denuncia invocara un perjuicio en el patrimonio de las Administraciones Públicas la no iniciación del procedimiento deberá ser motivada y se notificará a los denunciantes la decisión de si se ha iniciado o no el procedimiento.

4. Cuando el denunciante haya participado en la comisión de una infracción de esta naturaleza y existan otros infractores, el órgano competente para resolver el procedimiento deberá eximir al denunciante del pago de la multa que le correspondería u otro tipo de sanción de carácter no pecuniario, cuando sea el primero en aportar elementos de prueba que permitan iniciar el procedimiento o comprobar la infracción, siempre y cuando en el momento de aportarse aquellos no se disponga de elementos suficientes para ordenar la misma y se repare el perjuicio causado.

Asimismo, el órgano competente para resolver deberá reducir el importe del pago de la multa que le correspondería o, en su caso, la sanción de carácter no pecuniario, cuando no cumpliéndose alguna de las condiciones anteriores, el denunciante facilite elementos de prueba que aporten un valor añadido significativo respecto de aquellos de los que se disponga.

En ambos casos será necesario que el denunciante cese en la participación de la infracción y no haya destruido elementos de prueba relacionados con el objeto de la denuncia.

5. La presentación de una denuncia no confiere, por sí sola, la condición de interesado en el procedimiento.

Artículo 63. *Especialidades en el inicio de los procedimientos de naturaleza sancionadora.*

1. Los procedimientos de naturaleza sancionadora se iniciarán siempre de oficio por acuerdo del órgano competente y establecerán la debida separación entre la fase instructora y la sancionadora, que se encomendará a órganos distintos.

Se considerará que un órgano es competente para iniciar el procedimiento cuando así lo determinen las normas reguladoras del mismo.

2. En ningún caso se podrá imponer una sanción sin que se haya tramitado el oportuno procedimiento.

3. No se podrán iniciar nuevos procedimientos de carácter sancionador por hechos o conductas tipificadas como infracciones en cuya comisión el infractor persista de forma continuada, en tanto no haya recaído una primera resolución sancionadora, con carácter ejecutivo.

Artículo 64. *Acuerdo de iniciación en los procedimientos de naturaleza sancionadora.*

1. El acuerdo de iniciación se comunicará al instructor del procedimiento, con traslado de cuantas actuaciones existan al respecto, y se notificará a los interesados, entendiendo en todo caso por tal al inculpado.

Asimismo, la incoación se comunicará al denunciante cuando las normas reguladoras del procedimiento así lo prevean.

2. El acuerdo de iniciación deberá contener al menos:

a) Identificación de la persona o personas presuntamente responsables.

b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Identificación del instructor y, en su caso, Secretario del procedimiento, con expresa indicación del régimen de recusación de los mismos.

d) Órgano competente para la resolución del procedimiento y norma que le atribuya tal competencia, indicando la posibilidad de que el presunto responsable pueda reconocer voluntariamente su responsabilidad, con los efectos previstos en el artículo 85.

e) Medidas de carácter provisional que se hayan acordado por el órgano competente para iniciar el procedimiento sancionador, sin perjuicio de las que se puedan adoptar durante el mismo de conformidad con el artículo 56.

f) Indicación del derecho a formular alegaciones y a la audiencia en el procedimiento y de los plazos para su ejercicio, así como indicación de que, en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada.

3. Excepcionalmente, cuando en el momento de dictar el acuerdo de iniciación no existan elementos suficientes para la calificación inicial de los hechos que motivan la incoación del procedimiento, la citada calificación podrá realizarse en una fase posterior mediante la elaboración de un Pliego de cargos, que deberá ser notificado a los interesados.

Artículo 65. *Especialidades en el inicio de oficio de los procedimientos de responsabilidad patrimonial.*

1. Cuando las Administraciones Públicas decidan iniciar de oficio un procedimiento de responsabilidad patrimonial será necesario que no haya prescrito el derecho a la reclamación del interesado al que se refiere el artículo 67.

2. El acuerdo de iniciación del procedimiento se notificará a los particulares presuntamente lesionados, concediéndoles un plazo de diez días para que aporten cuantas alegaciones, documentos o información estimen conveniente a su derecho y propongan cuantas pruebas sean pertinentes para el reconocimiento del mismo. El procedimiento iniciado se instruirá aunque los particulares presuntamente lesionados no se personen en el plazo establecido.

Sección 3.ª Inicio del procedimiento a solicitud del interesado

Artículo 66. *Solicitudes de iniciación.*

1. Las solicitudes que se formulen deberán contener:

a) Nombre y apellidos del interesado y, en su caso, de la persona que lo represente.

b) Identificación del medio electrónico, o en su defecto, lugar físico en que desea que se practique la notificación. Adicionalmente, los interesados podrán aportar su dirección de correo electrónico y/o dispositivo electrónico con el fin de que las Administraciones Públicas les avisen del envío o puesta a disposición de la notificación.

c) Hechos, razones y petición en que se concrete, con toda claridad, la solicitud.

d) Lugar y fecha.

e) Firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio.

f) Órgano, centro o unidad administrativa a la que se dirige y su correspondiente código de identificación.

Las oficinas de asistencia en materia de registros estarán obligadas a facilitar a los interesados el código de identificación si el interesado lo desconoce. Asimismo, las Administraciones Públicas deberán mantener y actualizar en la sede electrónica correspondiente un listado con los códigos de identificación vigentes.

2. Cuando las pretensiones correspondientes a una pluralidad de personas tengan un contenido y fundamento idéntico o sustancialmente similar, podrán ser formuladas en una única solicitud, salvo que las normas reguladoras de los procedimientos específicos dispongan otra cosa.

3. De las solicitudes, comunicaciones y escritos que presenten los interesados electrónicamente o en las oficinas de asistencia en materia de registros de la Administración, podrán éstos exigir el correspondiente recibo que acredite la fecha y hora de presentación.

4. Las Administraciones Públicas deberán establecer modelos y sistemas de presentación masiva que permitan a los interesados presentar simultáneamente varias solicitudes. Estos modelos, de uso voluntario, estarán a disposición de los interesados en las correspondientes sedes electrónicas y en las oficinas de asistencia en materia de registros de las Administraciones Públicas.

Los solicitantes podrán acompañar los elementos que estimen convenientes para precisar o completar los datos del modelo, los cuales deberán ser admitidos y tenidos en cuenta por el órgano al que se dirijan.

5. Los sistemas normalizados de solicitud podrán incluir comprobaciones automáticas de la información aportada respecto de datos almacenados en sistemas propios o pertenecientes a otras Administraciones u ofrecer el formulario cumplimentado, en todo o en parte, con objeto de que el interesado verifique la información y, en su caso, la modifique y complete.

6. Cuando la Administración en un procedimiento concreto establezca expresamente modelos específicos de presentación de solicitudes, éstos serán de uso obligatorio por los interesados.

Artículo 67. *Solicitudes de iniciación en los procedimientos de responsabilidad patrimonial.*

1. Los interesados sólo podrán solicitar el inicio de un procedimiento de responsabilidad patrimonial, cuando no haya prescrito su derecho a reclamar. El derecho a reclamar prescribirá al año de producido el hecho o el acto que motive la indemnización o se manifieste su efecto lesivo. En caso de daños de carácter físico o psíquico a las personas, el plazo empezará a computarse desde la curación o la determinación del alcance de las secuelas.

En los casos en que proceda reconocer derecho a indemnización por anulación en vía administrativa o contencioso-administrativa de un acto o disposición de carácter general, el derecho a reclamar prescribirá al año de haberse notificado la resolución administrativa o la sentencia definitiva.

En los casos de responsabilidad patrimonial a que se refiere el artículo 32, apartados 4 y 5, de la Ley de Régimen Jurídico del Sector Público, el derecho a reclamar prescribirá al año de la publicación en el «Boletín Oficial del Estado» o en el «Diario Oficial de la Unión Europea», según el caso, de la sentencia que declare la inconstitucionalidad de la norma o su carácter contrario al Derecho de la Unión Europea.

2. Además de lo previsto en el artículo 66, en la solicitud que realicen los interesados se deberán especificar las lesiones producidas, la presunta relación de causalidad entre éstas y el funcionamiento del servicio público, la evaluación económica de la responsabilidad patrimonial, si fuera posible, y el momento en que la lesión efectivamente se produjo, e irá acompañada de cuantas alegaciones, documentos e informaciones se estimen oportunos y de la proposición de prueba, concretando los medios de que pretenda valerse el reclamante.

Artículo 68. *Subsanación y mejora de la solicitud.*

1. Si la solicitud de iniciación no reúne los requisitos que señala el artículo 66, y, en su caso, los que señala el artículo 67 u otros exigidos por la legislación específica aplicable, se requerirá al interesado para que, en un plazo de diez días, subsane la falta o acompañe los documentos preceptivos, con indicación de que, si así no lo hiciera, se le tendrá por desistido de su petición, previa resolución que deberá ser dictada en los términos previstos en el artículo 21.

2. Siempre que no se trate de procedimientos selectivos o de concurrencia competitiva, este plazo podrá ser ampliado prudencialmente, hasta cinco días, a petición del interesado o a iniciativa del órgano, cuando la aportación de los documentos requeridos presente dificultades especiales.

3. En los procedimientos iniciados a solicitud de los interesados, el órgano competente podrá recabar del solicitante la modificación o mejora voluntarias de los términos de aquélla. De ello se levantará acta sucinta, que se incorporará al procedimiento.

4. Si alguno de los sujetos a los que hace referencia el artículo 14.2 y 14.3 presenta su solicitud presencialmente, las Administraciones Públicas requerirán al interesado para que la

subsane a través de su presentación electrónica. A estos efectos, se considerará como fecha de presentación de la solicitud aquella en la que haya sido realizada la subsanación.

Artículo 69. *Declaración responsable y comunicación.*

1. A los efectos de esta Ley, se entenderá por declaración responsable el documento suscrito por un interesado en el que éste manifiesta, bajo su responsabilidad, que cumple con los requisitos establecidos en la normativa vigente para obtener el reconocimiento de un derecho o facultad o para su ejercicio, que dispone de la documentación que así lo acredita, que la pondrá a disposición de la Administración cuando le sea requerida, y que se compromete a mantener el cumplimiento de las anteriores obligaciones durante el período de tiempo inherente a dicho reconocimiento o ejercicio.

Los requisitos a los que se refiere el párrafo anterior deberán estar recogidos de manera expresa, clara y precisa en la correspondiente declaración responsable. Las Administraciones podrán requerir en cualquier momento que se aporte la documentación que acredite el cumplimiento de los mencionados requisitos y el interesado deberá aportarla.

2. A los efectos de esta Ley, se entenderá por comunicación aquel documento mediante el que los interesados ponen en conocimiento de la Administración Pública competente sus datos identificativos o cualquier otro dato relevante para el inicio de una actividad o el ejercicio de un derecho.

3. Las declaraciones responsables y las comunicaciones permitirán, el reconocimiento o ejercicio de un derecho o bien el inicio de una actividad, desde el día de su presentación, sin perjuicio de las facultades de comprobación, control e inspección que tengan atribuidas las Administraciones Públicas.

No obstante lo dispuesto en el párrafo anterior, la comunicación podrá presentarse dentro de un plazo posterior al inicio de la actividad cuando la legislación correspondiente lo prevea expresamente.

4. La inexactitud, falsedad u omisión, de carácter esencial, de cualquier dato o información que se incorpore a una declaración responsable o a una comunicación, o la no presentación ante la Administración competente de la declaración responsable, la documentación que sea en su caso requerida para acreditar el cumplimiento de lo declarado, o la comunicación, determinará la imposibilidad de continuar con el ejercicio del derecho o actividad afectada desde el momento en que se tenga constancia de tales hechos, sin perjuicio de las responsabilidades penales, civiles o administrativas a que hubiera lugar.

Asimismo, la resolución de la Administración Pública que declare tales circunstancias podrá determinar la obligación del interesado de restituir la situación jurídica al momento previo al reconocimiento o al ejercicio del derecho o al inicio de la actividad correspondiente, así como la imposibilidad de instar un nuevo procedimiento con el mismo objeto durante un período de tiempo determinado por la ley, todo ello conforme a los términos establecidos en las normas sectoriales de aplicación.

5. Las Administraciones Públicas tendrán permanentemente publicados y actualizados modelos de declaración responsable y de comunicación, fácilmente accesibles a los interesados.

6. Únicamente será exigible, bien una declaración responsable, bien una comunicación para iniciar una misma actividad u obtener el reconocimiento de un mismo derecho o facultad para su ejercicio, sin que sea posible la exigencia de ambas acumulativamente.

CAPÍTULO III

Ordenación del procedimiento

Artículo 70. *Expediente Administrativo.*

1. Se entiende por expediente administrativo el conjunto ordenado de documentos y actuaciones que sirven de antecedente y fundamento a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

2. Los expedientes tendrán formato electrónico y se formarán mediante la agregación ordenada de cuantos documentos, pruebas, dictámenes, informes, acuerdos, notificaciones y demás diligencias deban integrarlos, así como un índice numerado de todos los

documentos que contenga cuando se remita. Asimismo, deberá constar en el expediente copia electrónica certificada de la resolución adoptada.

3. Cuando en virtud de una norma sea preciso remitir el expediente electrónico, se hará de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en las correspondientes Normas Técnicas de Interoperabilidad, y se enviará completo, foliado, autentificado y acompañado de un índice, asimismo autentificado, de los documentos que contenga. La autenticación del citado índice garantizará la integridad e inmutabilidad del expediente electrónico generado desde el momento de su firma y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes electrónicos.

4. No formará parte del expediente administrativo la información que tenga carácter auxiliar o de apoyo, como la contenida en aplicaciones, ficheros y bases de datos informáticas, notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas, así como los juicios de valor emitidos por las Administraciones Públicas, salvo que se trate de informes, preceptivos y facultativos, solicitados antes de la resolución administrativa que ponga fin al procedimiento.

Artículo 71. *Impulso.*

1. El procedimiento, sometido al principio de celeridad, se impulsará de oficio en todos sus trámites y a través de medios electrónicos, respetando los principios de transparencia y publicidad.

2. En el despacho de los expedientes se guardará el orden riguroso de incoación en asuntos de homogénea naturaleza, salvo que por el titular de la unidad administrativa se dé orden motivada en contrario, de la que quede constancia.

El incumplimiento de lo dispuesto en el párrafo anterior dará lugar a la exigencia de responsabilidad disciplinaria del infractor y, en su caso, será causa de remoción del puesto de trabajo.

3. Las personas designadas como órgano instructor o, en su caso, los titulares de las unidades administrativas que tengan atribuida tal función serán responsables directos de la tramitación del procedimiento y, en especial, del cumplimiento de los plazos establecidos.

Artículo 72. *Concentración de trámites.*

1. De acuerdo con el principio de simplificación administrativa, se acordarán en un solo acto todos los trámites que, por su naturaleza, admitan un impulso simultáneo y no sea obligado su cumplimiento sucesivo.

2. Al solicitar los trámites que deban ser cumplidos por otros órganos, deberá consignarse en la comunicación cursada el plazo legal establecido al efecto.

Artículo 73. *Cumplimiento de trámites.*

1. Los trámites que deban ser cumplimentados por los interesados deberán realizarse en el plazo de diez días a partir del siguiente al de la notificación del correspondiente acto, salvo en el caso de que en la norma correspondiente se fije plazo distinto.

2. En cualquier momento del procedimiento, cuando la Administración considere que alguno de los actos de los interesados no reúne los requisitos necesarios, lo pondrá en conocimiento de su autor, concediéndole un plazo de diez días para cumplimentarlo.

3. A los interesados que no cumplan lo dispuesto en los apartados anteriores, se les podrá declarar decaídos en su derecho al trámite correspondiente. No obstante, se admitirá la actuación del interesado y producirá sus efectos legales, si se produjera antes o dentro del día que se notifique la resolución en la que se tenga por transcurrido el plazo.

Artículo 74. *Cuestiones incidentales.*

Las cuestiones incidentales que se susciten en el procedimiento, incluso las que se refieran a la nulidad de actuaciones, no suspenderán la tramitación del mismo, salvo la recusación.

CAPÍTULO IV

Instrucción del procedimiento

Sección 1.ª Disposiciones generales

Artículo 75. *Actos de instrucción.*

1. Los actos de instrucción necesarios para la determinación, conocimiento y comprobación de los hechos en virtud de los cuales deba pronunciarse la resolución, se realizarán de oficio y a través de medios electrónicos, por el órgano que tramite el procedimiento, sin perjuicio del derecho de los interesados a proponer aquellas actuaciones que requieran su intervención o constituyan trámites legal o reglamentariamente establecidos.

2. Las aplicaciones y sistemas de información utilizados para la instrucción de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación de los órganos responsables y la tramitación ordenada de los expedientes, así como facilitar la simplificación y la publicidad de los procedimientos.

3. Los actos de instrucción que requieran la intervención de los interesados habrán de practicarse en la forma que resulte más conveniente para ellos y sea compatible, en la medida de lo posible, con sus obligaciones laborales o profesionales.

4. En cualquier caso, el órgano instructor adoptará las medidas necesarias para lograr el pleno respeto a los principios de contradicción y de igualdad de los interesados en el procedimiento.

Artículo 76. *Alegaciones.*

1. Los interesados podrán, en cualquier momento del procedimiento anterior al trámite de audiencia, aducir alegaciones y aportar documentos u otros elementos de juicio.

Unos y otros serán tenidos en cuenta por el órgano competente al redactar la correspondiente propuesta de resolución.

2. En todo momento podrán los interesados alegar los defectos de tramitación y, en especial, los que supongan paralización, infracción de los plazos preceptivamente señalados o la omisión de trámites que pueden ser subsanados antes de la resolución definitiva del asunto. Dichas alegaciones podrán dar lugar, si hubiere razones para ello, a la exigencia de la correspondiente responsabilidad disciplinaria.

Sección 2.ª Prueba

Artículo 77. *Medios y período de prueba.*

1. Los hechos relevantes para la decisión de un procedimiento podrán acreditarse por cualquier medio de prueba admisible en Derecho, cuya valoración se realizará de acuerdo con los criterios establecidos en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

2. Cuando la Administración no tenga por ciertos los hechos alegados por los interesados o la naturaleza del procedimiento lo exija, el instructor del mismo acordará la apertura de un período de prueba por un plazo no superior a treinta días ni inferior a diez, a fin de que puedan practicarse cuantas juzgue pertinentes. Asimismo, cuando lo considere necesario, el instructor, a petición de los interesados, podrá decidir la apertura de un período extraordinario de prueba por un plazo no superior a diez días.

3. El instructor del procedimiento sólo podrá rechazar las pruebas propuestas por los interesados cuando sean manifiestamente improcedentes o innecesarias, mediante resolución motivada.

3 bis. Cuando el interesado alegue discriminación y aporte indicios fundados sobre su existencia, corresponderá a la persona a quien se impute la situación discriminatoria la aportación de una justificación objetiva y razonable, suficientemente probada, de las medidas adoptadas y de su proporcionalidad.

A los efectos de lo dispuesto en el párrafo anterior, el órgano administrativo podrá recabar informe de los organismos públicos competentes en materia de igualdad.

4. En los procedimientos de carácter sancionador, los hechos declarados probados por resoluciones judiciales penales firmes vincularán a las Administraciones Públicas respecto de los procedimientos sancionadores que substancien.

5. Los documentos formalizados por los funcionarios a los que se reconoce la condición de autoridad y en los que, observándose los requisitos legales correspondientes se recojan los hechos constatados por aquéllos harán prueba de éstos salvo que se acredite lo contrario.

6. Cuando la prueba consista en la emisión de un informe de un órgano administrativo, organismo público o Entidad de derecho público, se entenderá que éste tiene carácter preceptivo.

7. Cuando la valoración de las pruebas practicadas pueda constituir el fundamento básico de la decisión que se adopte en el procedimiento, por ser pieza imprescindible para la correcta evaluación de los hechos, deberá incluirse en la propuesta de resolución.

Artículo 78. *Práctica de prueba.*

1. La Administración comunicará a los interesados, con antelación suficiente, el inicio de las actuaciones necesarias para la realización de las pruebas que hayan sido admitidas.

2. En la notificación se consignará el lugar, fecha y hora en que se practicará la prueba, con la advertencia, en su caso, de que el interesado puede nombrar técnicos para que le asistan.

3. En los casos en que, a petición del interesado, deban efectuarse pruebas cuya realización implique gastos que no deba soportar la Administración, ésta podrá exigir el anticipo de los mismos, a reserva de la liquidación definitiva, una vez practicada la prueba. La liquidación de los gastos se practicará uniendo los comprobantes que acrediten la realidad y cuantía de los mismos.

Sección 3.ª Informes

Artículo 79. *Petición.*

1. A efectos de la resolución del procedimiento, se solicitarán aquellos informes que sean preceptivos por las disposiciones legales, y los que se juzguen necesarios para resolver, citándose el precepto que los exija o fundamentando, en su caso, la conveniencia de reclamarlos.

2. En la petición de informe se concretará el extremo o extremos acerca de los que se solicita.

Artículo 80. *Emisión de informes.*

1. Salvo disposición expresa en contrario, los informes serán facultativos y no vinculantes.

2. Los informes serán emitidos a través de medios electrónicos y de acuerdo con los requisitos que señala el artículo 26 en el plazo de diez días, salvo que una disposición o el cumplimiento del resto de los plazos del procedimiento permita o exija otro plazo mayor o menor.

3. De no emitirse el informe en el plazo señalado, y sin perjuicio de la responsabilidad en que incurra el responsable de la demora, se podrán proseguir las actuaciones salvo cuando se trate de un informe preceptivo, en cuyo caso se podrá suspender el transcurso del plazo máximo legal para resolver el procedimiento en los términos establecidos en la letra d) del apartado 1 del artículo 22.

4. Si el informe debiera ser emitido por una Administración Pública distinta de la que tramita el procedimiento en orden a expresar el punto de vista correspondiente a sus competencias respectivas, y transcurriera el plazo sin que aquél se hubiera emitido, se podrán proseguir las actuaciones.

El informe emitido fuera de plazo podrá no ser tenido en cuenta al adoptar la correspondiente resolución.

Artículo 81. *Solicitud de informes y dictámenes en los procedimientos de responsabilidad patrimonial.*

1. En el caso de los procedimientos de responsabilidad patrimonial será preceptivo solicitar informe al servicio cuyo funcionamiento haya ocasionado la presunta lesión indemnizable, no pudiendo exceder de diez días el plazo de su emisión.

2. Cuando las indemnizaciones reclamadas sean de cuantía igual o superior a 50.000 euros o a la que se establezca en la correspondiente legislación autonómica, así como en aquellos casos que disponga la Ley Orgánica 3/1980, de 22 de abril, del Consejo de Estado, será preceptivo solicitar dictamen del Consejo de Estado o, en su caso, del órgano consultivo de la Comunidad Autónoma.

A estos efectos, el órgano instructor, en el plazo de diez días a contar desde la finalización del trámite de audiencia, remitirá al órgano competente para solicitar el dictamen una propuesta de resolución, que se ajustará a lo previsto en el artículo 91, o, en su caso, la propuesta de acuerdo por el que se podría terminar convencionalmente el procedimiento.

El dictamen se emitirá en el plazo de dos meses y deberá pronunciarse sobre la existencia o no de relación de causalidad entre el funcionamiento del servicio público y la lesión producida y, en su caso, sobre la valoración del daño causado y la cuantía y modo de la indemnización de acuerdo con los criterios establecidos en esta Ley.

3. En el caso de reclamaciones en materia de responsabilidad patrimonial del Estado por el funcionamiento anormal de la Administración de Justicia, será preceptivo el informe del Consejo General del Poder Judicial que será evacuado en el plazo máximo de dos meses. El plazo para dictar resolución quedará suspendido por el tiempo que medie entre la solicitud del informe y su recepción, no pudiendo exceder dicho plazo de los citados dos meses.

Sección 4.ª Participación de los interesados

Artículo 82. *Trámite de audiencia.*

1. Instruidos los procedimientos, e inmediatamente antes de redactar la propuesta de resolución, se pondrán de manifiesto a los interesados o, en su caso, a sus representantes, para lo que se tendrán en cuenta las limitaciones previstas en su caso en la Ley 19/2013, de 9 de diciembre.

La audiencia a los interesados será anterior a la solicitud del informe del órgano competente para el asesoramiento jurídico o a la solicitud del Dictamen del Consejo de Estado u órgano consultivo equivalente de la Comunidad Autónoma, en el caso que éstos formaran parte del procedimiento.

2. Los interesados, en un plazo no inferior a diez días ni superior a quince, podrán alegar y presentar los documentos y justificaciones que estimen pertinentes.

3. Si antes del vencimiento del plazo los interesados manifiestan su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite.

4. Se podrá prescindir del trámite de audiencia cuando no figuren en el procedimiento ni sean tenidos en cuenta en la resolución otros hechos ni otras alegaciones y pruebas que las aducidas por el interesado.

5. En los procedimientos de responsabilidad patrimonial a los que se refiere el artículo 32.9 de la Ley de Régimen Jurídico del Sector Público, será necesario en todo caso dar audiencia al contratista, notificándole cuantas actuaciones se realicen en el procedimiento, al efecto de que se persone en el mismo, exponga lo que a su derecho convenga y proponga cuantos medios de prueba estime necesarios.

Artículo 83. *Información pública.*

1. El órgano al que corresponda la resolución del procedimiento, cuando la naturaleza de éste lo requiera, podrá acordar un período de información pública.

2. A tal efecto, se publicará un anuncio en el Diario oficial correspondiente a fin de que cualquier persona física o jurídica pueda examinar el expediente, o la parte del mismo que se acuerde.

El anuncio señalará el lugar de exhibición, debiendo estar en todo caso a disposición de las personas que lo soliciten a través de medios electrónicos en la sede electrónica correspondiente, y determinará el plazo para formular alegaciones, que en ningún caso podrá ser inferior a veinte días.

3. La incomparecencia en este trámite no impedirá a los interesados interponer los recursos procedentes contra la resolución definitiva del procedimiento.

La comparecencia en el trámite de información pública no otorga, por sí misma, la condición de interesado. No obstante, quienes presenten alegaciones u observaciones en este trámite tienen derecho a obtener de la Administración una respuesta razonada, que podrá ser común para todas aquellas alegaciones que planteen cuestiones sustancialmente iguales.

4. Conforme a lo dispuesto en las leyes, las Administraciones Públicas podrán establecer otras formas, medios y cauces de participación de las personas, directamente o a través de las organizaciones y asociaciones reconocidas por la ley en el procedimiento en el que se dictan los actos administrativos.

CAPÍTULO V

Finalización del procedimiento

Sección 1.ª Disposiciones generales

Artículo 84. *Terminación.*

1. Pondrán fin al procedimiento la resolución, el desistimiento, la renuncia al derecho en que se funde la solicitud, cuando tal renuncia no esté prohibida por el ordenamiento jurídico, y la declaración de caducidad.

2. También producirá la terminación del procedimiento la imposibilidad material de continuarlo por causas sobrevenidas. La resolución que se dicte deberá ser motivada en todo caso.

Artículo 85. *Terminación en los procedimientos sancionadores.*

1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente.

Artículo 86. *Terminación convencional.*

1. Las Administraciones Públicas podrán celebrar acuerdos, pactos, convenios o contratos con personas tanto de Derecho público como privado, siempre que no sean contrarios al ordenamiento jurídico ni versen sobre materias no susceptibles de transacción y tengan por objeto satisfacer el interés público que tienen encomendado, con el alcance, efectos y régimen jurídico específico que, en su caso, prevea la disposición que lo regule, pudiendo tales actos tener la consideración de finalizadores de los procedimientos

administrativos o insertarse en los mismos con carácter previo, vinculante o no, a la resolución que les ponga fin.

2. Los citados instrumentos deberán establecer como contenido mínimo la identificación de las partes intervinientes, el ámbito personal, funcional y territorial, y el plazo de vigencia, debiendo publicarse o no según su naturaleza y las personas a las que estuvieran destinados.

3. Requerirán en todo caso la aprobación expresa del Consejo de Ministros u órgano equivalente de las Comunidades Autónomas, los acuerdos que versen sobre materias de la competencia directa de dicho órgano.

4. Los acuerdos que se suscriban no supondrán alteración de las competencias atribuidas a los órganos administrativos, ni de las responsabilidades que correspondan a las autoridades y funcionarios, relativas al funcionamiento de los servicios públicos.

5. En los casos de procedimientos de responsabilidad patrimonial, el acuerdo alcanzado entre las partes deberá fijar la cuantía y modo de indemnización de acuerdo con los criterios que para calcularla y abonarla establece el artículo 34 de la Ley de Régimen Jurídico del Sector Público.

Sección 2.ª Resolución

Artículo 87. *Actuaciones complementarias.*

Antes de dictar resolución, el órgano competente para resolver podrá decidir, mediante acuerdo motivado, la realización de las actuaciones complementarias indispensables para resolver el procedimiento. No tendrán la consideración de actuaciones complementarias los informes que preceden inmediatamente a la resolución final del procedimiento.

El acuerdo de realización de actuaciones complementarias se notificará a los interesados, concediéndoseles un plazo de siete días para formular las alegaciones que tengan por pertinentes tras la finalización de las mismas. Las actuaciones complementarias deberán practicarse en un plazo no superior a quince días. El plazo para resolver el procedimiento quedará suspendido hasta la terminación de las actuaciones complementarias.

Artículo 88. *Contenido.*

1. La resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

Cuando se trate de cuestiones conexas que no hubieran sido planteadas por los interesados, el órgano competente podrá pronunciarse sobre las mismas, poniéndolo antes de manifiesto a aquéllos por un plazo no superior a quince días, para que formulen las alegaciones que estimen pertinentes y aporten, en su caso, los medios de prueba.

2. En los procedimientos tramitados a solicitud del interesado, la resolución será congruente con las peticiones formuladas por éste, sin que en ningún caso pueda agravar su situación inicial y sin perjuicio de la potestad de la Administración de incoar de oficio un nuevo procedimiento, si procede.

3. Las resoluciones contendrán la decisión, que será motivada en los casos a que se refiere el artículo 35. Expresarán, además, los recursos que contra la misma procedan, órgano administrativo o judicial ante el que hubieran de presentarse y plazo para interponerlos, sin perjuicio de que los interesados puedan ejercitar cualquier otro que estimen oportuno.

4. Sin perjuicio de la forma y lugar señalados por el interesado para la práctica de las notificaciones, la resolución del procedimiento se dictará electrónicamente y garantizará la identidad del órgano competente, así como la autenticidad e integridad del documento que se formalice mediante el empleo de alguno de los instrumentos previstos en esta Ley.

5. En ningún caso podrá la Administración abstenerse de resolver so pretexto de silencio, oscuridad o insuficiencia de los preceptos legales aplicables al caso, aunque podrá acordarse la inadmisión de las solicitudes de reconocimiento de derechos no previstos en el ordenamiento jurídico o manifiestamente carentes de fundamento, sin perjuicio del derecho de petición previsto por el artículo 29 de la Constitución.

6. La aceptación de informes o dictámenes servirá de motivación a la resolución cuando se incorporen al texto de la misma.

7. Cuando la competencia para instruir y resolver un procedimiento no recaiga en un mismo órgano, será necesario que el instructor eleve al órgano competente para resolver una propuesta de resolución.

En los procedimientos de carácter sancionador, la propuesta de resolución deberá ser notificada a los interesados en los términos previstos en el artículo siguiente.

Artículo 89. *Propuesta de resolución en los procedimientos de carácter sancionador.*

1. El órgano instructor resolverá la finalización del procedimiento, con archivo de las actuaciones, sin que sea necesaria la formulación de la propuesta de resolución, cuando en la instrucción procedimiento se ponga de manifiesto que concurre alguna de las siguientes circunstancias:

a) La inexistencia de los hechos que pudieran constituir la infracción.

b) Cuando los hechos no resulten acreditados.

c) Cuando los hechos probados no constituyan, de modo manifiesto, infracción administrativa.

d) Cuando no exista o no se haya podido identificar a la persona o personas responsables o bien aparezcan exentos de responsabilidad.

e) Cuando se concluyera, en cualquier momento, que ha prescrito la infracción.

2. En el caso de procedimientos de carácter sancionador, una vez concluida la instrucción del procedimiento, el órgano instructor formulará una propuesta de resolución que deberá ser notificada a los interesados. La propuesta de resolución deberá indicar la puesta de manifiesto del procedimiento y el plazo para formular alegaciones y presentar los documentos e informaciones que se estimen pertinentes.

3. En la propuesta de resolución se fijarán de forma motivada los hechos que se consideren probados y su exacta calificación jurídica, se determinará la infracción que, en su caso, aquéllos constituyan, la persona o personas responsables y la sanción que se proponga, la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión, así como las medidas provisionales que, en su caso, se hubieran adoptado. Cuando la instrucción concluya la inexistencia de infracción o responsabilidad y no se haga uso de la facultad prevista en el apartado primero, la propuesta declarará esa circunstancia.

Artículo 90. *Especialidades de la resolución en los procedimientos sancionadores.*

1. En el caso de procedimientos de carácter sancionador, además del contenido previsto en los dos artículos anteriores, la resolución incluirá la valoración de las pruebas practicadas, en especial aquellas que constituyan los fundamentos básicos de la decisión, fijarán los hechos y, en su caso, la persona o personas responsables, la infracción o infracciones cometidas y la sanción o sanciones que se imponen, o bien la declaración de no existencia de infracción o responsabilidad.

2. En la resolución no se podrán aceptar hechos distintos de los determinados en el curso del procedimiento, con independencia de su diferente valoración jurídica. No obstante, cuando el órgano competente para resolver considere que la infracción o la sanción revisten mayor gravedad que la determinada en la propuesta de resolución, se notificará al inculpado para que aporte cuantas alegaciones estime convenientes en el plazo de quince días.

3. La resolución que ponga fin al procedimiento será ejecutiva cuando no quepa contra ella ningún recurso ordinario en vía administrativa, pudiendo adoptarse en la misma las disposiciones cautelares precisas para garantizar su eficacia en tanto no sea ejecutiva y que podrán consistir en el mantenimiento de las medidas provisionales que en su caso se hubieran adoptado.

Cuando la resolución sea ejecutiva, se podrá suspender cautelarmente, si el interesado manifiesta a la Administración su intención de interponer recurso contencioso-administrativo contra la resolución firme en vía administrativa. Dicha suspensión cautelar finalizará cuando:

a) Haya transcurrido el plazo legalmente previsto sin que el interesado haya interpuesto recurso contencioso-administrativo.

b) Habiendo el interesado interpuesto recurso contencioso-administrativo:

1.º No se haya solicitado en el mismo trámite la suspensión cautelar de la resolución impugnada.

2.º El órgano judicial se pronuncie sobre la suspensión cautelar solicitada, en los términos previstos en ella.

4. Cuando las conductas sancionadas hubieran causado daños o perjuicios a las Administraciones y la cuantía destinada a indemnizar estos daños no hubiera quedado determinada en el expediente, se fijará mediante un procedimiento complementario, cuya resolución será inmediatamente ejecutiva. Este procedimiento será susceptible de terminación convencional, pero ni ésta ni la aceptación por el infractor de la resolución que pudiera recaer implicarán el reconocimiento voluntario de su responsabilidad. La resolución del procedimiento pondrá fin a la vía administrativa.

Artículo 91. *Especialidades de la resolución en los procedimientos en materia de responsabilidad patrimonial.*

1. Una vez recibido, en su caso, el dictamen al que se refiere el artículo 81.2 o, cuando éste no sea preceptivo, una vez finalizado el trámite de audiencia, el órgano competente resolverá o someterá la propuesta de acuerdo para su formalización por el interesado y por el órgano administrativo competente para suscribirlo. Cuando no se estimase procedente formalizar la propuesta de terminación convencional, el órgano competente resolverá en los términos previstos en el apartado siguiente.

2. Además de lo previsto en el artículo 88, en los casos de procedimientos de responsabilidad patrimonial, será necesario que la resolución se pronuncie sobre la existencia o no de la relación de causalidad entre el funcionamiento del servicio público y la lesión producida y, en su caso, sobre la valoración del daño causado, la cuantía y el modo de la indemnización, cuando proceda, de acuerdo con los criterios que para calcularla y abonarla se establecen en el artículo 34 de la Ley de Régimen Jurídico del Sector Público.

3. Transcurridos seis meses desde que se inició el procedimiento sin que haya recaído y se notifique resolución expresa o, en su caso, se haya formalizado el acuerdo, podrá entenderse que la resolución es contraria a la indemnización del particular.

Artículo 92. *Competencia para la resolución de los procedimientos de responsabilidad patrimonial.*

En el ámbito de la Administración General del Estado, los procedimientos de responsabilidad patrimonial se resolverán por el Ministro respectivo o por el Consejo de Ministros en los casos del artículo 32.3 de la Ley de Régimen Jurídico del Sector Público o cuando una ley así lo disponga.

En el ámbito autonómico y local, los procedimientos de responsabilidad patrimonial se resolverán por los órganos correspondientes de las Comunidades Autónomas o de las Entidades que integran la Administración Local.

En el caso de las Entidades de Derecho Público, las normas que determinen su régimen jurídico podrán establecer los órganos a quien corresponde la resolución de los procedimientos de responsabilidad patrimonial. En su defecto, se aplicarán las normas previstas en este artículo.

Sección 3.ª Desistimiento y renuncia

Artículo 93. *Desistimiento por la Administración.*

En los procedimientos iniciados de oficio, la Administración podrá desistir, motivadamente, en los supuestos y con los requisitos previstos en las Leyes.

Artículo 94. *Desistimiento y renuncia por los interesados.*

1. Todo interesado podrá desistir de su solicitud o, cuando ello no esté prohibido por el ordenamiento jurídico, renunciar a sus derechos.

2. Si el escrito de iniciación se hubiera formulado por dos o más interesados, el desistimiento o la renuncia sólo afectará a aquellos que la hubiesen formulado.

3. Tanto el desistimiento como la renuncia podrán hacerse por cualquier medio que permita su constancia, siempre que incorpore las firmas que correspondan de acuerdo con lo previsto en la normativa aplicable.

4. La Administración aceptará de plano el desistimiento o la renuncia, y declarará concluso el procedimiento salvo que, habiéndose personado en el mismo terceros interesados, instasen éstos su continuación en el plazo de diez días desde que fueron notificados del desistimiento o renuncia.

5. Si la cuestión suscitada por la incoación del procedimiento entrañase interés general o fuera conveniente sustanciarla para su definición y esclarecimiento, la Administración podrá limitar los efectos del desistimiento o la renuncia al interesado y seguirá el procedimiento.

Sección 4.ª Caducidad

Artículo 95. *Requisitos y efectos.*

1. En los procedimientos iniciados a solicitud del interesado, cuando se produzca su paralización por causa imputable al mismo, la Administración le advertirá que, transcurridos tres meses, se producirá la caducidad del procedimiento. Consumido este plazo sin que el particular requerido realice las actividades necesarias para reanudar la tramitación, la Administración acordará el archivo de las actuaciones, notificándoselo al interesado. Contra la resolución que declare la caducidad procederán los recursos pertinentes.

2. No podrá acordarse la caducidad por la simple inactividad del interesado en la cumplimentación de trámites, siempre que no sean indispensables para dictar resolución. Dicha inactividad no tendrá otro efecto que la pérdida de su derecho al referido trámite.

3. La caducidad no producirá por sí sola la prescripción de las acciones del particular o de la Administración, pero los procedimientos caducados no interrumpirán el plazo de prescripción.

En los casos en los que sea posible la iniciación de un nuevo procedimiento por no haberse producido la prescripción, podrán incorporarse a éste los actos y trámites cuyo contenido se hubiera mantenido igual de no haberse producido la caducidad. En todo caso, en el nuevo procedimiento deberán cumplimentarse los trámites de alegaciones, proposición de prueba y audiencia al interesado.

4. Podrá no ser aplicable la caducidad en el supuesto de que la cuestión suscitada afecte al interés general, o fuera conveniente sustanciarla para su definición y esclarecimiento.

CAPÍTULO VI

De la tramitación simplificada del procedimiento administrativo común

Artículo 96. *Tramitación simplificada del procedimiento administrativo común.*

1. Cuando razones de interés público o la falta de complejidad del procedimiento así lo aconsejen, las Administraciones Públicas podrán acordar, de oficio o a solicitud del interesado, la tramitación simplificada del procedimiento.

En cualquier momento del procedimiento anterior a su resolución, el órgano competente para su tramitación podrá acordar continuar con arreglo a la tramitación ordinaria.

2. Cuando la Administración acuerde de oficio la tramitación simplificada del procedimiento deberá notificarlo a los interesados. Si alguno de ellos manifestara su oposición expresa, la Administración deberá seguir la tramitación ordinaria.

3. Los interesados podrán solicitar la tramitación simplificada del procedimiento. Si el órgano competente para la tramitación aprecia que no concurre alguna de las razones previstas en el apartado 1, podrá desestimar dicha solicitud, en el plazo de cinco días desde

su presentación, sin que exista posibilidad de recurso por parte del interesado. Transcurrido el mencionado plazo de cinco días se entenderá desestimada la solicitud.

4. En el caso de procedimientos en materia de responsabilidad patrimonial de las Administraciones Públicas, si una vez iniciado el procedimiento administrativo el órgano competente para su tramitación considera inequívoca la relación de causalidad entre el funcionamiento del servicio público y la lesión, así como la valoración del daño y el cálculo de la cuantía de la indemnización, podrá acordar de oficio la suspensión del procedimiento general y la iniciación de un procedimiento simplificado.

5. En el caso de procedimientos de naturaleza sancionadora, se podrá adoptar la tramitación simplificada del procedimiento cuando el órgano competente para iniciar el procedimiento considere que, de acuerdo con lo previsto en su normativa reguladora, existen elementos de juicio suficientes para calificar la infracción como leve, sin que quepa la oposición expresa por parte del interesado prevista en el apartado 2.

6. Salvo que reste menos para su tramitación ordinaria, los procedimientos administrativos tramitados de manera simplificada deberán ser resueltos en treinta días, a contar desde el siguiente al que se notifique al interesado el acuerdo de tramitación simplificada del procedimiento, y constarán únicamente de los siguientes trámites:

a) Inicio del procedimiento de oficio o a solicitud del interesado.

b) Subsanación de la solicitud presentada, en su caso.

c) Alegaciones formuladas al inicio del procedimiento durante el plazo de cinco días.

d) Trámite de audiencia, únicamente cuando la resolución vaya a ser desfavorable para el interesado.

e) Informe del servicio jurídico, cuando éste sea preceptivo.

f) Informe del Consejo General del Poder Judicial, cuando éste sea preceptivo.

g) Dictamen del Consejo de Estado u órgano consultivo equivalente de la Comunidad Autónoma en los casos en que sea preceptivo. Desde que se solicite el Dictamen al Consejo de Estado, u órgano equivalente, hasta que éste sea emitido, se producirá la suspensión automática del plazo para resolver.

El órgano competente solicitará la emisión del Dictamen en un plazo tal que permita cumplir el plazo de resolución del procedimiento. El Dictamen podrá ser emitido en el plazo de quince días si así lo solicita el órgano competente.

En todo caso, en el expediente que se remita al Consejo de Estado u órgano consultivo equivalente, se incluirá una propuesta de resolución. Cuando el Dictamen sea contrario al fondo de la propuesta de resolución, con independencia de que se atienda o no este criterio, el órgano competente para resolver acordará continuar el procedimiento con arreglo a la tramitación ordinaria, lo que se notificará a los interesados. En este caso, se entenderán convalidadas todas las actuaciones que se hubieran realizado durante la tramitación simplificada del procedimiento, a excepción del Dictamen del Consejo de Estado u órgano consultivo equivalente.

h) Resolución.

7. En el caso que un procedimiento exigiera la realización de un trámite no previsto en el apartado anterior, deberá ser tramitado de manera ordinaria.

CAPÍTULO VII

Ejecución

Artículo 97. *Título.*

1. Las Administraciones Públicas no iniciarán ninguna actuación material de ejecución de resoluciones que limite derechos de los particulares sin que previamente haya sido adoptada la resolución que le sirva de fundamento jurídico.

2. El órgano que ordene un acto de ejecución material de resoluciones estará obligado a notificar al particular interesado la resolución que autorice la actuación administrativa.

Artículo 98. *Ejecutoriedad.*

1. Los actos de las Administraciones Públicas sujetos al Derecho Administrativo serán inmediatamente ejecutivos, salvo que:

a) Se produzca la suspensión de la ejecución del acto.
b) Se trate de una resolución de un procedimiento de naturaleza sancionadora contra la que quepa algún recurso en vía administrativa, incluido el potestativo de reposición.
c) Una disposición establezca lo contrario.
d) Se necesite aprobación o autorización superior.

2. Cuando de una resolución administrativa, o de cualquier otra forma de finalización del procedimiento administrativo prevista en esta ley, nazca una obligación de pago derivada de una sanción pecuniaria, multa o cualquier otro derecho que haya de abonarse a la Hacienda pública, éste se efectuará preferentemente, salvo que se justifique la imposibilidad de hacerlo, utilizando alguno de los medios electrónicos siguientes:

a) Tarjeta de crédito y débito.
b) Transferencia bancaria.
c) Domiciliación bancaria.
d) Cualesquiera otros que se autoricen por el órgano competente en materia de Hacienda Pública.

Artículo 99. *Ejecución forzosa.*

Las Administraciones Públicas, a través de sus órganos competentes en cada caso, podrán proceder, previo apercibimiento, a la ejecución forzosa de los actos administrativos, salvo en los supuestos en que se suspenda la ejecución de acuerdo con la Ley, o cuando la Constitución o la Ley exijan la intervención de un órgano judicial.

Artículo 100. *Medios de ejecución forzosa.*

1. La ejecución forzosa por las Administraciones Públicas se efectuará, respetando siempre el principio de proporcionalidad, por los siguientes medios:

a) Apremio sobre el patrimonio.
b) Ejecución subsidiaria.
c) Multa coercitiva.
d) Compulsión sobre las personas.

2. Si fueran varios los medios de ejecución admisibles se elegirá el menos restrictivo de la libertad individual.
3. Si fuese necesario entrar en el domicilio del afectado o en los restantes lugares que requieran la autorización de su titular, las Administraciones Públicas deberán obtener el consentimiento del mismo o, en su defecto, la oportuna autorización judicial.

Artículo 101. *Apremio sobre el patrimonio.*

1. Si en virtud de acto administrativo hubiera de satisfacerse cantidad líquida se seguirá el procedimiento previsto en las normas reguladoras del procedimiento de apremio.
2. En cualquier caso no podrá imponerse a los administrados una obligación pecuniaria que no estuviese establecida con arreglo a una norma de rango legal.

Artículo 102. *Ejecución subsidiaria.*

1. Habrá lugar a la ejecución subsidiaria cuando se trate de actos que por no ser personalísimos puedan ser realizados por sujeto distinto del obligado.
2. En este caso, las Administraciones Públicas realizarán el acto, por sí o a través de las personas que determinen, a costa del obligado.
3. El importe de los gastos, daños y perjuicios se exigirá conforme a lo dispuesto en el artículo anterior.
4. Dicho importe podrá liquidarse de forma provisional y realizarse antes de la ejecución, a reserva de la liquidación definitiva.

Artículo 103. *Multa coercitiva.*

1. Cuando así lo autoricen las Leyes, y en la forma y cuantía que éstas determinen, las Administraciones Públicas pueden, para la ejecución de determinados actos, imponer multas coercitivas, reiteradas por lapsos de tiempo que sean suficientes para cumplir lo ordenado, en los siguientes supuestos:

a) Actos personalísimos en que no proceda la compulsión directa sobre la persona del obligado.
b) Actos en que, procediendo la compulsión, la Administración no la estimara conveniente.
c) Actos cuya ejecución pueda el obligado encargar a otra persona.

2. La multa coercitiva es independiente de las sanciones que puedan imponerse con tal carácter y compatible con ellas.

Artículo 104. *Compulsión sobre las personas.*

1. Los actos administrativos que impongan una obligación personalísima de no hacer o soportar podrán ser ejecutados por compulsión directa sobre las personas en los casos en que la ley expresamente lo autorice, y dentro siempre del respeto debido a su dignidad y a los derechos reconocidos en la Constitución.
2. Si, tratándose de obligaciones personalísimas de hacer, no se realizase la prestación, el obligado deberá resarcir los daños y perjuicios, a cuya liquidación y cobro se procederá en vía administrativa.

Artículo 105. *Prohibición de acciones posesorias.*

No se admitirán a trámite acciones posesorias contra las actuaciones de los órganos administrativos realizadas en materia de su competencia y de acuerdo con el procedimiento legalmente establecido.

TÍTULO V

De la revisión de los actos en vía administrativa

CAPÍTULO I

Revisión de oficio

Artículo 106. *Revisión de disposiciones y actos nulos.*

1. Las Administraciones Públicas, en cualquier momento, por iniciativa propia o a solicitud de interesado, y previo dictamen favorable del Consejo de Estado u órgano consultivo equivalente de la Comunidad Autónoma, si lo hubiere, declararán de oficio la nulidad de los actos administrativos que hayan puesto fin a la vía administrativa o que no hayan sido recurridos en plazo, en los supuestos previstos en el artículo 47.1.
2. Asimismo, en cualquier momento, las Administraciones Públicas de oficio, y previo dictamen favorable del Consejo de Estado u órgano consultivo equivalente de la Comunidad Autónoma si lo hubiere, podrán declarar la nulidad de las disposiciones administrativas en los supuestos previstos en el artículo 47.2.
3. El órgano competente para la revisión de oficio podrá acordar motivadamente la inadmisión a trámite de las solicitudes formuladas por los interesados, sin necesidad de recabar Dictamen del Consejo de Estado u órgano consultivo de la Comunidad Autónoma, cuando las mismas no se basen en alguna de las causas de nulidad del artículo 47.1 o carezcan manifiestamente de fundamento, así como en el supuesto de que se hubieran desestimado en cuanto al fondo otras solicitudes sustancialmente iguales.
4. Las Administraciones Públicas, al declarar la nulidad de una disposición o acto, podrán establecer, en la misma resolución, las indemnizaciones que proceda reconocer a los interesados, si se dan las circunstancias previstas en los artículos 32.2 y 34.1 de la Ley de

Régimen Jurídico del Sector Público sin perjuicio de que, tratándose de una disposición, subsistan los actos firmes dictados en aplicación de la misma.

5. Cuando el procedimiento se hubiera iniciado de oficio, el transcurso del plazo de seis meses desde su inicio sin dictarse resolución producirá la caducidad del mismo. Si el procedimiento se hubiera iniciado a solicitud de interesado, se podrá entender la misma desestimada por silencio administrativo.

Artículo 107. *Declaración de lesividad de actos anulables.*

1. Las Administraciones Públicas podrán impugnar ante el orden jurisdiccional contencioso-administrativo los actos favorables para los interesados que sean anulables conforme a lo dispuesto en el artículo 48, previa su declaración de lesividad para el interés público.

2. La declaración de lesividad no podrá adoptarse una vez transcurridos cuatro años desde que se dictó el acto administrativo y exigirá la previa audiencia de cuantos aparezcan como interesados en el mismo, en los términos establecidos por el artículo 82.

Sin perjuicio de su examen como presupuesto procesal de admisibilidad de la acción en el proceso judicial correspondiente, la declaración de lesividad no será susceptible de recurso, si bien podrá notificarse a los interesados a los meros efectos informativos.

3. Transcurrido el plazo de seis meses desde la iniciación del procedimiento sin que se hubiera declarado la lesividad, se producirá la caducidad del mismo.

4. Si el acto proviniera de la Administración General del Estado o de las Comunidades Autónomas, la declaración de lesividad se adoptará por el órgano de cada Administración competente en la materia.

5. Si el acto proviniera de las entidades que integran la Administración Local, la declaración de lesividad se adoptará por el Pleno de la Corporación o, en defecto de éste, por el órgano colegiado superior de la entidad.

Artículo 108. *Suspensión.*

Iniciado el procedimiento de revisión de oficio al que se refieren los artículos 106 y 107, el órgano competente para declarar la nulidad o lesividad, podrá suspender la ejecución del acto, cuando ésta pudiera causar perjuicios de imposible o difícil reparación.

Artículo 109. *Revocación de actos y rectificación de errores.*

1. Las Administraciones Públicas podrán revocar, mientras no haya transcurrido el plazo de prescripción, sus actos de gravamen o desfavorables, siempre que tal revocación no constituya dispensa o exención no permitida por las leyes, ni sea contraria al principio de igualdad, al interés público o al ordenamiento jurídico.

2. Las Administraciones Públicas podrán, asimismo, rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos existentes en sus actos.

Artículo 110. *Límites de la revisión.*

Las facultades de revisión establecidas en este Capítulo, no podrán ser ejercidas cuando por prescripción de acciones, por el tiempo transcurrido o por otras circunstancias, su ejercicio resulte contrario a la equidad, a la buena fe, al derecho de los particulares o a las leyes.

Artículo 111. *Competencia para la revisión de oficio de las disposiciones y de actos nulos y anulables en la Administración General del Estado.*

En el ámbito estatal, serán competentes para la revisión de oficio de las disposiciones y los actos administrativos nulos y anulables:

a) El Consejo de Ministros, respecto de sus propios actos y disposiciones y de los actos y disposiciones dictados por los Ministros.

b) En la Administración General del Estado:

1.º Los Ministros, respecto de los actos y disposiciones de los Secretarios de Estado y de los dictados por órganos directivos de su Departamento no dependientes de una Secretaría de Estado.

2.º Los Secretarios de Estado, respecto de los actos y disposiciones dictados por los órganos directivos de ellos dependientes.

c) En los Organismos públicos y entidades de derecho público vinculados o dependientes de la Administración General del Estado:

1.º Los órganos a los que estén adscritos los Organismos públicos y entidades de derecho público, respecto de los actos y disposiciones dictados por el máximo órgano rector de éstos.

2.º Los máximos órganos rectores de los Organismos públicos y entidades de derecho público, respecto de los actos y disposiciones dictados por los órganos de ellos dependientes.

CAPÍTULO II

Recursos administrativos

Sección 1.ª Principios generales

Artículo 112. *Objeto y clases.*

1. Contra las resoluciones y los actos de trámite, si estos últimos deciden directa o indirectamente el fondo del asunto, determinan la imposibilidad de continuar el procedimiento, producen indefensión o perjuicio irreparable a derechos e intereses legítimos, podrán interponerse por los interesados los recursos de alzada y potestativo de reposición, que cabrá fundar en cualquiera de los motivos de nulidad o anulabilidad previstos en los artículos 47 y 48 de esta Ley.

La oposición a los restantes actos de trámite podrá alegarse por los interesados para su consideración en la resolución que ponga fin al procedimiento.

2. Las leyes podrán sustituir el recurso de alzada, en supuestos o ámbitos sectoriales determinados, y cuando la especificidad de la materia así lo justifique, por otros procedimientos de impugnación, reclamación, conciliación, mediación y arbitraje, ante órganos colegiados o Comisiones específicas no sometidas a instrucciones jerárquicas, con respeto a los principios, garantías y plazos que la presente Ley reconoce a las personas y a los interesados en todo procedimiento administrativo.

En las mismas condiciones, el recurso de reposición podrá ser sustituido por los procedimientos a que se refiere el párrafo anterior, respetando su carácter potestativo para el interesado.

La aplicación de estos procedimientos en el ámbito de la Administración Local no podrá suponer el desconocimiento de las facultades resolutorias reconocidas a los órganos representativos electos establecidos por la Ley.

3. Contra las disposiciones administrativas de carácter general no cabrá recurso en vía administrativa.

Los recursos contra un acto administrativo que se funden únicamente en la nulidad de alguna disposición administrativa de carácter general podrán interponerse directamente ante el órgano que dictó dicha disposición.

4. Las reclamaciones económico-administrativas se ajustarán a los procedimientos establecidos por su legislación específica.

Artículo 113. *Recurso extraordinario de revisión.*

Contra los actos firmes en vía administrativa, sólo procederá el recurso extraordinario de revisión cuando concurra alguna de las circunstancias previstas en el artículo 125.1.

Artículo 114. *Fin de la vía administrativa.*

1. Ponen fin a la vía administrativa:

a) Las resoluciones de los recursos de alzada.
b) Las resoluciones de los procedimientos a que se refiere el artículo 112.2.
c) Las resoluciones de los órganos administrativos que carezcan de superior jerárquico, salvo que una Ley establezca lo contrario.
d) Los acuerdos, pactos, convenios o contratos que tengan la consideración de finalizadores del procedimiento.
e) La resolución administrativa de los procedimientos de responsabilidad patrimonial, cualquiera que fuese el tipo de relación, pública o privada, de que derive.
f) La resolución de los procedimientos complementarios en materia sancionadora a los que se refiere el artículo 90.4.
g) Las demás resoluciones de órganos administrativos cuando una disposición legal o reglamentaria así lo establezca.

2. Además de lo previsto en el apartado anterior, en el ámbito estatal ponen fin a la vía administrativa los actos y resoluciones siguientes:

a) Los actos administrativos de los miembros y órganos del Gobierno.
b) Los emanados de los Ministros y los Secretarios de Estado en el ejercicio de las competencias que tienen atribuidas los órganos de los que son titulares.
c) Los emanados de los órganos directivos con nivel de Director general o superior, en relación con las competencias que tengan atribuidas en materia de personal.
d) En los Organismos públicos y entidades de derecho público vinculados o dependientes de la Administración General del Estado, los emanados de los máximos órganos de dirección unipersonales o colegiados, de acuerdo con lo que establezcan sus estatutos, salvo que por ley se establezca otra cosa.

Artículo 115. *Interposición de recurso.*

1. La interposición del recurso deberá expresar:

a) El nombre y apellidos del recurrente, así como la identificación personal del mismo.
b) El acto que se recurre y la razón de su impugnación.
c) Lugar, fecha, firma del recurrente, identificación del medio y, en su caso, del lugar que se señale a efectos de notificaciones.
d) Órgano, centro o unidad administrativa al que se dirige y su correspondiente código de identificación.
e) Las demás particularidades exigidas, en su caso, por las disposiciones específicas.

2. El error o la ausencia de la calificación del recurso por parte del recurrente no será obstáculo para su tramitación, siempre que se deduzca su verdadero carácter.
3. Los vicios y defectos que hagan anulable un acto no podrán ser alegados por quienes los hubieren causado.

Artículo 116. *Causas de inadmisión.*

Serán causas de inadmisión las siguientes:

a) Ser incompetente el órgano administrativo, cuando el competente perteneciera a otra Administración Pública. El recurso deberá remitirse al órgano competente, de acuerdo con lo establecido en el artículo 14.1 de la Ley de Régimen Jurídico del Sector Público.
b) Carecer de legitimación el recurrente.
c) Tratarse de un acto no susceptible de recurso.
d) Haber transcurrido el plazo para la interposición del recurso.
e) Carecer el recurso manifiestamente de fundamento.

Artículo 117. *Suspensión de la ejecución.*

1. La interposición de cualquier recurso, excepto en los casos en que una disposición establezca lo contrario, no suspenderá la ejecución del acto impugnado.
2. No obstante lo dispuesto en el apartado anterior, el órgano a quien competa resolver el recurso, previa ponderación, suficientemente razonada, entre el perjuicio que causaría al interés público o a terceros la suspensión y el ocasionado al recurrente como consecuencia

de la eficacia inmediata del acto recurrido, podrá suspender, de oficio o a solicitud del recurrente, la ejecución del acto impugnado cuando concurran alguna de las siguientes circunstancias:

a) Que la ejecución pudiera causar perjuicios de imposible o difícil reparación.

b) Que la impugnación se fundamente en alguna de las causas de nulidad de pleno derecho previstas en el artículo 47.1 de esta Ley.

3. La ejecución del acto impugnado se entenderá suspendida si transcurrido un mes desde que la solicitud de suspensión haya tenido entrada en el registro electrónico de la Administración u Organismo competente para decidir sobre la misma, el órgano a quien competa resolver el recurso no ha dictado y notificado resolución expresa al respecto. En estos casos, no será de aplicación lo establecido en el artículo 21.4 segundo párrafo, de esta Ley.

4. Al dictar el acuerdo de suspensión podrán adoptarse las medidas cautelares que sean necesarias para asegurar la protección del interés público o de terceros y la eficacia de la resolución o el acto impugnado.

Cuando de la suspensión puedan derivarse perjuicios de cualquier naturaleza, aquélla sólo producirá efectos previa prestación de caución o garantía suficiente para responder de ellos, en los términos establecidos reglamentariamente.

La suspensión se prolongará después de agotada la vía administrativa cuando, habiéndolo solicitado previamente el interesado, exista medida cautelar y los efectos de ésta se extiendan a la vía contencioso-administrativa. Si el interesado interpusiera recurso contencioso-administrativo, solicitando la suspensión del acto objeto del proceso, se mantendrá la suspensión hasta que se produzca el correspondiente pronunciamiento judicial sobre la solicitud.

5. Cuando el recurso tenga por objeto la impugnación de un acto administrativo que afecte a una pluralidad indeterminada de personas, la suspensión de su eficacia habrá de ser publicada en el periódico oficial en que aquél se insertó.

Artículo 118. *Audiencia de los interesados.*

1. Cuando hayan de tenerse en cuenta nuevos hechos o documentos no recogidos en el expediente originario, se pondrán de manifiesto a los interesados para que, en un plazo no inferior a diez días ni superior a quince, formulen las alegaciones y presenten los documentos y justificantes que estimen procedentes.

No se tendrán en cuenta en la resolución de los recursos, hechos, documentos o alegaciones del recurrente, cuando habiendo podido aportarlos en el trámite de alegaciones no lo haya hecho. Tampoco podrá solicitarse la práctica de pruebas cuando su falta de realización en el procedimiento en el que se dictó la resolución recurrida fuera imputable al interesado.

2. Si hubiera otros interesados se les dará, en todo caso, traslado del recurso para que en el plazo antes citado, aleguen cuanto estimen procedente.

3. El recurso, los informes y las propuestas no tienen el carácter de documentos nuevos a los efectos de este artículo. Tampoco lo tendrán los que los interesados hayan aportado al expediente antes de recaer la resolución impugnada.

Artículo 119. *Resolución.*

1. La resolución del recurso estimará en todo o en parte o desestimará las pretensiones formuladas en el mismo o declarará su inadmisión.

2. Cuando existiendo vicio de forma no se estime procedente resolver sobre el fondo se ordenará la retroacción del procedimiento al momento en el que el vicio fue cometido, sin perjuicio de que eventualmente pueda acordarse la convalidación de actuaciones por el órgano competente para ello, de acuerdo con lo dispuesto en el artículo 52.

3. El órgano que resuelva el recurso decidirá cuantas cuestiones, tanto de forma como de fondo, plantee el procedimiento, hayan sido o no alegadas por los interesados. En este último caso se les oirá previamente. No obstante, la resolución será congruente con las peticiones formuladas por el recurrente, sin que en ningún caso pueda agravarse su situación inicial.

Artículo 120. *Pluralidad de recursos administrativos.*

1. Cuando deban resolverse una pluralidad de recursos administrativos que traigan causa de un mismo acto administrativo y se hubiera interpuesto un recurso judicial contra una resolución administrativa o bien contra el correspondiente acto presunto desestimatorio, el órgano administrativo podrá acordar la suspensión del plazo para resolver hasta que recaiga pronunciamiento judicial.

2. El acuerdo de suspensión deberá ser notificado a los interesados, quienes podrán recurrirlo.

La interposición del correspondiente recurso por un interesado, no afectará a los restantes procedimientos de recurso que se encuentren suspendidos por traer causa del mismo acto administrativo.

3. Recaído el pronunciamiento judicial, será comunicado a los interesados y el órgano administrativo competente para resolver podrá dictar resolución sin necesidad de realizar ningún trámite adicional, salvo el de audiencia, cuando proceda.

Sección 2.ª Recurso de alzada

Artículo 121. *Objeto.*

1. Las resoluciones y actos a que se refiere el artículo 112.1, cuando no pongan fin a la vía administrativa, podrán ser recurridos en alzada ante el órgano superior jerárquico del que los dictó. A estos efectos, los Tribunales y órganos de selección del personal al servicio de las Administraciones Públicas y cualesquiera otros que, en el seno de éstas, actúen con autonomía funcional, se considerarán dependientes del órgano al que estén adscritos o, en su defecto, del que haya nombrado al presidente de los mismos.

2. El recurso podrá interponerse ante el órgano que dictó el acto que se impugna o ante el competente para resolverlo.

Si el recurso se hubiera interpuesto ante el órgano que dictó el acto impugnado, éste deberá remitirlo al competente en el plazo de diez días, con su informe y con una copia completa y ordenada del expediente.

El titular del órgano que dictó el acto recurrido será responsable directo del cumplimiento de lo previsto en el párrafo anterior.

Artículo 122. *Plazos.*

1. El plazo para la interposición del recurso de alzada será de un mes, si el acto fuera expreso. Transcurrido dicho plazo sin haberse interpuesto el recurso, la resolución será firme a todos los efectos.

Si el acto no fuera expreso el solicitante y otros posibles interesados podrán interponer recurso de alzada en cualquier momento a partir del día siguiente a aquel en que, de acuerdo con su normativa específica, se produzcan los efectos del silencio administrativo.

2. El plazo máximo para dictar y notificar la resolución será de tres meses. Transcurrido este plazo sin que recaiga resolución, se podrá entender desestimado el recurso, salvo en el supuesto previsto en el artículo 24.1, tercer párrafo.

3. Contra la resolución de un recurso de alzada no cabrá ningún otro recurso administrativo, salvo el recurso extraordinario de revisión, en los casos establecidos en el artículo 125.1.

Sección 3.ª Recurso potestativo de reposición

Artículo 123. *Objeto y naturaleza.*

1. Los actos administrativos que pongan fin a la vía administrativa podrán ser recurridos potestativamente en reposición ante el mismo órgano que los hubiera dictado o ser impugnados directamente ante el orden jurisdiccional contencioso-administrativo.

2. No se podrá interponer recurso contencioso-administrativo hasta que sea resuelto expresamente o se haya producido la desestimación presunta del recurso de reposición interpuesto.

Artículo 124. *Plazos.*

1. El plazo para la interposición del recurso de reposición será de un mes, si el acto fuera expreso. Transcurrido dicho plazo, únicamente podrá interponerse recurso contencioso-administrativo, sin perjuicio, en su caso, de la procedencia del recurso extraordinario de revisión.

Si el acto no fuera expreso, el solicitante y otros posibles interesados podrán interponer recurso de reposición en cualquier momento a partir del día siguiente a aquel en que, de acuerdo con su normativa específica, se produzca el acto presunto.

2. El plazo máximo para dictar y notificar la resolución del recurso será de un mes.

3. Contra la resolución de un recurso de reposición no podrá interponerse de nuevo dicho recurso.

Sección 4.ª Recurso extraordinario de revisión

Artículo 125. *Objeto y plazos.*

1. Contra los actos firmes en vía administrativa podrá interponerse el recurso extraordinario de revisión ante el órgano administrativo que los dictó, que también será el competente para su resolución, cuando concurra alguna de las circunstancias siguientes:

a) Que al dictarlos se hubiera incurrido en error de hecho, que resulte de los propios documentos incorporados al expediente.

b) Que aparezcan documentos de valor esencial para la resolución del asunto que, aunque sean posteriores, evidencien el error de la resolución recurrida.

c) Que en la resolución hayan influido esencialmente documentos o testimonios declarados falsos por sentencia judicial firme, anterior o posterior a aquella resolución.

d) Que la resolución se hubiese dictado como consecuencia de prevaricación, cohecho, violencia, maquinación fraudulenta u otra conducta punible y se haya declarado así en virtud de sentencia judicial firme.

2. El recurso extraordinario de revisión se interpondrá, cuando se trate de la causa a) del apartado anterior, dentro del plazo de cuatro años siguientes a la fecha de la notificación de la resolución impugnada. En los demás casos, el plazo será de tres meses a contar desde el conocimiento de los documentos o desde que la sentencia judicial quedó firme.

3. Lo establecido en el presente artículo no perjudica el derecho de los interesados a formular la solicitud y la instancia a que se refieren los artículos 106 y 109.2 de la presente Ley ni su derecho a que las mismas se sustancien y resuelvan.

Artículo 126. *Resolución.*

1. El órgano competente para la resolución del recurso podrá acordar motivadamente la inadmisión a trámite, sin necesidad de recabar dictamen del Consejo de Estado u órgano consultivo de la Comunidad Autónoma, cuando el mismo no se funde en alguna de las causas previstas en el apartado 1 del artículo anterior o en el supuesto de que se hubiesen desestimado en cuanto al fondo otros recursos sustancialmente iguales.

2. El órgano al que corresponde conocer del recurso extraordinario de revisión debe pronunciarse no sólo sobre la procedencia del recurso, sino también, en su caso, sobre el fondo de la cuestión resuelta por el acto recurrido.

3. Transcurrido el plazo de tres meses desde la interposición del recurso extraordinario de revisión sin haberse dictado y notificado la resolución, se entenderá desestimado, quedando expedita la vía jurisdiccional contencioso-administrativa.

TÍTULO VI

De la iniciativa legislativa y de la potestad para dictar reglamentos y otras disposiciones

Artículo 127. *Iniciativa legislativa y potestad para dictar normas con rango de ley.*

El Gobierno de la Nación ejercerá la iniciativa legislativa prevista en la Constitución mediante la elaboración y aprobación de los anteproyectos de Ley y la ulterior remisión de los proyectos de ley a las Cortes Generales.

La iniciativa legislativa se ejercerá por los órganos de gobierno de las Comunidades Autónomas en los términos establecidos por la Constitución y sus respectivos Estatutos de Autonomía.

Asimismo, el Gobierno de la Nación podrá aprobar reales decretos-leyes y reales decretos legislativos en los términos previstos en la Constitución. Los respectivos órganos de gobierno de las Comunidades Autónomas podrán aprobar normas equivalentes a aquéllas en su ámbito territorial, de conformidad con lo establecido en la Constitución y en sus respectivos Estatutos de Autonomía.

Artículo 128. *Potestad reglamentaria.*

1. El ejercicio de la potestad reglamentaria corresponde al Gobierno de la Nación, a los órganos de Gobierno de las Comunidades Autónomas, de conformidad con lo establecido en sus respectivos Estatutos, y a los órganos de gobierno locales, de acuerdo con lo previsto en la Constitución, los Estatutos de Autonomía y la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

2. Los reglamentos y disposiciones administrativas no podrán vulnerar la Constitución o las leyes ni regular aquellas materias que la Constitución o los Estatutos de Autonomía reconocen de la competencia de las Cortes Generales o de las Asambleas Legislativas de las Comunidades Autónomas. Sin perjuicio de su función de desarrollo o colaboración con respecto a la ley, no podrán tipificar delitos, faltas o infracciones administrativas, establecer penas o sanciones, así como tributos, exacciones parafiscales u otras cargas o prestaciones personales o patrimoniales de carácter público.

3. Las disposiciones administrativas se ajustarán al orden de jerarquía que establezcan las leyes. Ninguna disposición administrativa podrá vulnerar los preceptos de otra de rango superior.

Artículo 129. *Principios de buena regulación.*

1. En el ejercicio de la iniciativa legislativa y la potestad reglamentaria, las Administraciones Públicas actuarán de acuerdo con los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia, y eficiencia. En la exposición de motivos o en el preámbulo, según se trate, respectivamente, de anteproyectos de ley o de proyectos de reglamento, quedará suficientemente justificada su adecuación a dichos principios.

2. En virtud de los principios de necesidad y eficacia, la iniciativa normativa debe estar justificada por una razón de interés general, basarse en una identificación clara de los fines perseguidos y ser el instrumento más adecuado para garantizar su consecución.

3. En virtud del principio de proporcionalidad, la iniciativa que se proponga deberá contener la regulación imprescindible para atender la necesidad a cubrir con la norma, tras constatar que no existen otras medidas menos restrictivas de derechos, o que impongan menos obligaciones a los destinatarios.

4. A fin de garantizar el principio de seguridad jurídica, la iniciativa normativa se ejercerá de manera coherente con el resto del ordenamiento jurídico, nacional y de la Unión Europea, para generar un marco normativo estable, predecible, integrado, claro y de certidumbre, que facilite su conocimiento y comprensión y, en consecuencia, la actuación y toma de decisiones de las personas y empresas.

Cuando en materia de procedimiento administrativo la iniciativa normativa establezca trámites adicionales o distintos a los contemplados en esta Ley, éstos deberán ser justificados atendiendo a la singularidad de la materia o a los fines perseguidos por la propuesta.

Las habilitaciones para el desarrollo reglamentario de una ley serán conferidas, con carácter general, al Gobierno **o Consejo de Gobierno respectivo**. La atribución directa a los titulares de los departamentos ministeriales **o de las consejerías del Gobierno**, o a otros órganos dependientes o subordinados de ellos, tendrá carácter excepcional y deberá justificarse en la ley habilitante.

Las leyes podrán habilitar directamente a Autoridades Independientes u otros organismos que tengan atribuida esta potestad para aprobar normas en desarrollo o aplicación de las mismas, cuando la naturaleza de la materia así lo exija.

5. En aplicación del principio de transparencia, las Administraciones Públicas posibilitarán el acceso sencillo, universal y actualizado a la normativa en vigor y los documentos propios de su proceso de elaboración, en los términos establecidos en el artículo 7 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno; definirán claramente los objetivos de las iniciativas normativas y su justificación en el preámbulo o exposición de motivos; y posibilitarán que los potenciales destinatarios tengan una participación activa en la elaboración de las normas.

6. En aplicación del principio de eficiencia, la iniciativa normativa debe evitar cargas administrativas innecesarias o accesorias y racionalizar, en su aplicación, la gestión de los recursos públicos.

7. Cuando la iniciativa normativa afecte a los gastos o ingresos públicos presentes o futuros, se deberán cuantificar y valorar sus repercusiones y efectos, y supeditarse al cumplimiento de los principios de estabilidad presupuestaria y sostenibilidad financiera.

> Téngase en cuenta que este artículo se declara contrario al orden constitucional de competencias en los términos del fundamento jurídico 7 b), salvo los párrafos segundo y tercero del apartado 4, y la inconstitucionalidad y nulidad de los incisos destacados en negrita del párrafo tercero del apartado 4, por Sentencia del TC 55/2018, de 24 de mayo. Ref. BOE-A-2018-8574

Artículo 130. *Evaluación normativa y adaptación de la normativa vigente a los principios de buena regulación.*

1. Las Administraciones Públicas revisarán periódicamente su normativa vigente para adaptarla a los principios de buena regulación y para comprobar la medida en que las normas en vigor han conseguido los objetivos previstos y si estaba justificado y correctamente cuantificado el coste y las cargas impuestas en ellas.

El resultado de la evaluación se plasmará en un informe que se hará público, con el detalle, periodicidad y por el órgano que determine la normativa reguladora de la Administración correspondiente.

2. Las Administraciones Públicas promoverán la aplicación de los principios de buena regulación y cooperarán para promocionar el análisis económico en la elaboración de las normas y, en particular, para evitar la introducción de restricciones injustificadas o desproporcionadas a la actividad económica.

> Téngase en cuenta que este artículo se declara contrario al orden constitucional de competencias en los términos del fundamento jurídico 7 b) por Sentencia del TC 55/2018, de 24 de mayo. Ref. BOE-A-2018-8574

Artículo 131. *Publicidad de las normas.*

Las normas con rango de ley, los reglamentos y disposiciones administrativas habrán de publicarse en el diario oficial correspondiente para que entren en vigor y produzcan efectos jurídicos. Adicionalmente, y de manera facultativa, las Administraciones Públicas podrán establecer otros medios de publicidad complementarios.

La publicación de los diarios o boletines oficiales en las sedes electrónicas de la Administración, Órgano, Organismo público o Entidad competente tendrá, en las condiciones y con las garantías que cada Administración Pública determine, los mismos efectos que los atribuidos a su edición impresa.

La publicación del «Boletín Oficial del Estado» en la sede electrónica del Organismo competente tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

Artículo 132. *Planificación normativa.*

1. Anualmente, las Administraciones Públicas harán público un Plan Normativo que contendrá las iniciativas legales o reglamentarias que vayan a ser elevadas para su aprobación en el año siguiente.

2. Una vez aprobado, el Plan Anual Normativo se publicará en el Portal de la Transparencia de la Administración Pública correspondiente.

Téngase en cuenta que este artículo se declara contrario al orden constitucional de competencias en los términos del fundamento jurídico 7 b) y 7 c) por Sentencia del TC 55/2018, de 24 de mayo. Ref. BOE-A-2018-8574

Artículo 133. *Participación de los ciudadanos en el procedimiento de elaboración de normas con rango de Ley y reglamentos.*

1. Con carácter previo a la elaboración del proyecto o anteproyecto de ley o de reglamento, se sustanciará una consulta pública, a través del portal web de la Administración competente en la que se recabará la opinión de los sujetos y de las organizaciones más representativas potencialmente afectados por la futura norma acerca de:

a) Los problemas que se pretenden solucionar con la iniciativa.
b) La necesidad y oportunidad de su aprobación.
c) Los objetivos de la norma.
d) Las posibles soluciones alternativas regulatorias y no regulatorias.

2. Sin perjuicio de la consulta previa a la redacción del texto de la iniciativa, cuando la norma afecte a los derechos e intereses legítimos de las personas, el centro directivo competente publicará el texto en el portal web correspondiente, con el objeto de dar audiencia a los ciudadanos afectados y recabar cuantas aportaciones adicionales puedan hacerse por otras personas o entidades. Asimismo, podrá también recabarse directamente la opinión de las organizaciones o asociaciones reconocidas por ley que agrupen o representen a las personas cuyos derechos o intereses legítimos se vieren afectados por la norma y cuyos fines guarden relación directa con su objeto.

3. La consulta, audiencia e información públicas reguladas en este artículo deberán realizarse de forma tal que los potenciales destinatarios de la norma y quienes realicen aportaciones sobre ella tengan la posibilidad de emitir su opinión, para lo cual deberán ponerse a su disposición los documentos necesarios, que serán claros, concisos y reunir toda la información precisa para poder pronunciarse sobre la materia.

4. Podrá prescindirse de los trámites de consulta, audiencia e información públicas previstos en este artículo en el caso de normas presupuestarias u organizativas de la Administración General del Estado, la Administración autonómica, la Administración local o de las organizaciones dependientes o vinculadas a éstas, o cuando concurran razones graves de interés público que lo justifiquen.

Cuando la propuesta normativa no tenga un impacto significativo en la actividad económica, no imponga obligaciones relevantes a los destinatarios o regule aspectos parciales de una materia, podrá omitirse la consulta pública regulada en el apartado primero. Si la normativa reguladora del ejercicio de la iniciativa legislativa o de la potestad

reglamentaria por una Administración prevé la tramitación urgente de estos procedimientos, la eventual excepción del trámite por esta circunstancia se ajustará a lo previsto en aquella.

Téngase en cuenta que este artículo se declara contrario al orden constitucional de competencias en los términos del fundamento jurídico 7 b) y, salvo el inciso de su apartado primero «Con carácter previo a la elaboración del proyecto o anteproyecto de ley o de reglamento, se sustanciará una consulta pública» y el primer párrafo de su apartado 4, en los términos del fundamento jurídico 7 c), por Sentencia del TC 55/2018, de 24 de mayo. Ref. BOE-A-2018-8574

Disposición adicional primera. *Especialidades por razón de materia.*

1. Los procedimientos administrativos regulados en leyes especiales por razón de la materia que no exijan alguno de los trámites previstos en esta Ley o regulen trámites adicionales o distintos se regirán, respecto a éstos, por lo dispuesto en dichas leyes especiales.

2. Las siguientes actuaciones y procedimientos se regirán por su normativa específica y supletoriamente por lo dispuesto en esta Ley:

a) Las actuaciones y procedimientos de aplicación de los tributos en materia tributaria y aduanera, así como su revisión en vía administrativa.

b) Las actuaciones y procedimientos de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y Desempleo.

c) Las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.

d) Las actuaciones y procedimientos en materia de extranjería y asilo.

Disposición adicional segunda. *Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado.*

Para cumplir con lo previsto en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración, las Comunidades Autónomas y las Entidades Locales podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas y registros establecidos al efecto por la Administración General del Estado. Su no adhesión, deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

En el caso que una Comunidad Autónoma o una Entidad Local justifique ante el Ministerio de Hacienda y Administraciones Públicas que puede prestar el servicio de un modo más eficiente, de acuerdo con los criterios previstos en el párrafo anterior, y opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad, y sus normas técnicas de desarrollo, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas.

Téngase en cuenta que se declara que el párrafo segundo no es inconstitucional interpretado en los términos del fundamento jurídico 11 f) por Sentencia del TC 55/2018, de 24 de mayo. Ref. BOE-A-2018-8574

Disposición adicional tercera. *Notificación por medio de anuncio publicado en el «Boletín Oficial del Estado».*

1. El «Boletín Oficial del Estado» pondrá a disposición de las diversas Administraciones Públicas, un sistema automatizado de remisión y gestión telemática para la publicación de los anuncios de notificación en el mismo previstos en el artículo 44 de esta Ley y en esta disposición adicional. Dicho sistema, que cumplirá con lo establecido en esta Ley, y su normativa de desarrollo, garantizará la celeridad de la publicación, su correcta y fiel inserción, así como la identificación del órgano remitente.

2. En aquellos procedimientos administrativos que cuenten con normativa específica, de concurrir los supuestos previstos en el artículo 44 de esta Ley, la práctica de la notificación se hará, en todo caso, mediante un anuncio publicado en el «Boletín Oficial del Estado», sin perjuicio de que previamente y con carácter facultativo pueda realizarse en la forma prevista por dicha normativa específica.

3. La publicación en el «Boletín Oficial del Estado» de los anuncios a que se refieren los dos párrafos anteriores se efectuará sin contraprestación económica alguna por parte de quienes la hayan solicitado.

Disposición adicional cuarta. *Oficinas de asistencia en materia de registros.*

Las Administraciones Públicas deberán mantener permanentemente actualizado en la correspondiente sede electrónica un directorio geográfico que permita al interesado identificar la oficina de asistencia en materia de registros más próxima a su domicilio.

Disposición adicional quinta. *Actuación administrativa de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos.*

La actuación administrativa de los órganos competentes del Congreso de los Diputados, del Senado, del Consejo General del Poder Judicial, del Tribunal Constitucional, del Tribunal de Cuentas, del Defensor del Pueblo, de las Asambleas Legislativas de las Comunidades Autónomas y de las instituciones autonómicas análogas al Tribunal de Cuentas y al Defensor del Pueblo, se regirá por lo previsto en su normativa específica, en el marco de los principios que inspiran la actuación administrativa de acuerdo con esta Ley.

Disposición adicional sexta. *Sistemas de identificación y firma previstos en los artículos 9.2 c) y 10.2 c).*

1. No obstante lo dispuesto en los artículos 9.2 c) y 10.2 c) de la presente Ley, en las relaciones de los interesados con los sujetos sometidos al ámbito de aplicación de esta Ley, no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea.

2. En todo caso, cualquier sistema de identificación basado en tecnología de registro distribuido que prevea la legislación estatal a que hace referencia el apartado anterior deberá contemplar asimismo que la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública.

Disposición adicional séptima.

La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital informará a la Conferencia Sectorial para asuntos de Seguridad Nacional de las resoluciones denegatorias de la autorización prevista en los artículos 9.2.c) y 10.2.c) de esta ley, que, en su caso, se hayan dictado en el plazo máximo de tres meses desde la adopción de la citada resolución.

Disposición adicional octava. *Resoluciones de Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital que establezcan las condiciones de uso de sistemas de identificación y/o firma no criptográfica.*

Cuando se trate de sistemas establecidos por medio de Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital para su ámbito competencial con objeto de determinar las circunstancias en las que un sistema de firma electrónica no basado en certificados electrónicos será considerado como válido en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado, sus organismos públicos y entidades de Derecho Público vinculados o dependientes, no será preciso el transcurso del plazo de dos meses para la eficacia jurídica del sistema a que se refiere el artículo 10.2.c) de la presente ley, adquiriendo eficacia jurídica al día siguiente de la publicación de la Resolución, salvo que esta disponga otra cosa.

Disposición transitoria primera. *Archivo de documentos.*

1. El archivo de los documentos correspondientes a procedimientos administrativos ya iniciados antes de la entrada en vigor de la presente Ley, se regirán por lo dispuesto en la normativa anterior.
2. Siempre que sea posible, los documentos en papel asociados a procedimientos administrativos finalizados antes de la entrada en vigor de esta Ley, deberán digitalizarse de acuerdo con los requisitos establecidos en la normativa reguladora aplicable.

Disposición transitoria segunda. *Registro electrónico y archivo electrónico único.*

Mientras no entren en vigor las previsiones relativas al registro electrónico y el archivo electrónico único, en el ámbito de la Administración General del Estado se aplicarán las siguientes reglas:

a) Durante el primer año, tras la entrada en vigor de la Ley, podrán mantenerse los registros y archivos existentes en el momento de la entrada en vigor de esta ley.
b) Durante el segundo año, tras la entrada en vigor de la Ley, se dispondrá como máximo, de un registro electrónico y un archivo electrónico por cada Ministerio, así como de un registro electrónico por cada Organismo público.

Disposición transitoria tercera. *Régimen transitorio de los procedimientos.*

a) A los procedimientos ya iniciados antes de la entrada en vigor de la Ley no les será de aplicación la misma, rigiéndose por la normativa anterior.
b) Los procedimientos de revisión de oficio iniciados después de la entrada en vigor de la presente Ley se sustanciarán por las normas establecidas en ésta.
c) Los actos y resoluciones dictados con posterioridad a la entrada en vigor de esta Ley se regirán, en cuanto al régimen de recursos, por las disposiciones de la misma.
d) Los actos y resoluciones pendientes de ejecución a la entrada en vigor de esta Ley se regirán para su ejecución por la normativa vigente cuando se dictaron.
e) A falta de previsiones expresas establecidas en las correspondientes disposiciones legales y reglamentarias, las cuestiones de Derecho transitorio que se susciten en materia de procedimiento administrativo se resolverán de acuerdo con los principios establecidos en los apartados anteriores.

Disposición transitoria cuarta. *Régimen transitorio de los archivos, registros y punto de acceso general.*

Mientras no entren en vigor las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, punto de acceso general electrónico de la Administración y archivo único electrónico, las Administraciones Públicas mantendrán los mismos canales, medios o sistemas electrónicos vigentes relativos a dichas materias, que permitan garantizar el derecho de las personas a relacionarse electrónicamente con las Administraciones.

Disposición transitoria quinta. *Procedimientos de responsabilidad patrimonial derivados de la declaración de inconstitucionalidad de una norma o su carácter contrario al Derecho de la Unión Europea.*

Los procedimientos administrativos de responsabilidad patrimonial derivados de la declaración de inconstitucionalidad de una norma o su carácter contrario al Derecho de la Unión Europea iniciados con anterioridad a la entrada en vigor de esta Ley, se resolverán de acuerdo con la normativa vigente en el momento de su iniciación.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en la presente Ley.

2. Quedan derogadas expresamente las siguientes disposiciones:

a) Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

b) Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

c) Los artículos 4 a 7 de la Ley 2/2011, de 4 de marzo, de Economía Sostenible.

d) Real Decreto 429/1993, de 26 de marzo, por el que se aprueba el Reglamento de los procedimientos de las Administraciones Públicas en materia de responsabilidad patrimonial.

e) Real Decreto 1398/1993, de 4 de agosto, por el que se aprueba el Reglamento del Procedimiento para el Ejercicio de la Potestad Sancionadora.

f) Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

g) Los artículos 2.3, 10, 13, 14, 15, 16, 26, 27, 28, 29.1.a), 29.1.d), 31, 32, 33, 35, 36, 39, 48, 50, los apartados 1, 2 y 4 de la disposición adicional primera, la disposición adicional tercera, la disposición transitoria primera, la disposición transitoria segunda, la disposición transitoria tercera y la disposición transitoria cuarta del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

Hasta que, de acuerdo con lo dispuesto en la disposición final séptima, produzcan efectos las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, punto de acceso general electrónico de la Administración y archivo único electrónico, se mantendrán en vigor los artículos de las normas previstas en las letras a), b) y g) relativos a las materias mencionadas.

3. Las referencias contenidas en normas vigentes a las disposiciones que se derogan expresamente deberán entenderse efectuadas a las disposiciones de esta Ley que regulan la misma materia que aquéllas.

Disposición final primera. *Título competencial.*

1. Esta Ley se aprueba al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española, que atribuye al Estado la competencia para dictar las bases del régimen jurídico de las Administraciones Públicas y competencia en materia de procedimiento administrativo común y sistema de responsabilidad de todas las Administraciones Públicas.

2. **(Anulado)**

3. Lo previsto en los artículos 92 primer párrafo, 111, 114.2 y disposición transitoria segunda, serán de aplicación únicamente a la Administración General del Estado, así como el resto de apartados de los distintos preceptos que prevén su aplicación exclusiva en el ámbito de la Administración General del Estado.

Disposición final segunda. *Modificación de la Ley 59/2003, de 19 de diciembre, de firma electrónica.*

En la Ley 59/2003, de 19 de diciembre, de firma electrónica, se incluye un nuevo apartado 11 en el artículo 3 con la siguiente redacción:

> «11. Todos los sistemas de identificación y firma electrónica previstos en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y en la Ley de Régimen Jurídico del Sector Público tendrán plenos efectos jurídicos.»

Disposición final tercera. *Modificación de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social.*

La Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social, queda redactada en los siguientes términos:

Uno. El artículo 64 queda redactado como sigue:

> **«Artículo 64.** *Excepciones a la conciliación o mediación previas.*
>
> 1. Se exceptúan del requisito del intento de conciliación o, en su caso, de mediación los procesos que exijan el agotamiento de la vía administrativa, en su caso, los que versen sobre Seguridad Social, los relativos a la impugnación del despido colectivo por los representantes de los trabajadores, disfrute de vacaciones y a materia electoral, movilidad geográfica, modificación sustancial de las condiciones de trabajo, suspensión del contrato y reducción de jornada por causas económicas, técnicas, organizativas o de producción o derivadas de fuerza mayor, derechos de conciliación de la vida personal, familiar y laboral a los que se refiere el artículo 139, los iniciados de oficio, los de impugnación de convenios colectivos, los de impugnación de los estatutos de los sindicatos o de su modificación, los de tutela de los derechos fundamentales y libertades públicas, los procesos de anulación de laudos arbitrales, los de impugnación de acuerdos de conciliaciones, de mediaciones y de transacciones, así como aquellos en que se ejerciten acciones laborales de protección contra la violencia de género.
>
> 2. Igualmente, quedan exceptuados:
>
> a) Aquellos procesos en los que siendo parte demandada el Estado u otro ente público también lo fueren personas privadas, siempre que la pretensión hubiera de someterse al agotamiento de la vía administrativa y en ésta pudiera decidirse el asunto litigioso.
>
> b) Los supuestos en que, en cualquier momento del proceso, después de haber dirigido la papeleta o la demanda contra personas determinadas, fuera necesario dirigir o ampliar la misma frente a personas distintas de las inicialmente demandadas.
>
> 3. Cuando por la naturaleza de la pretensión ejercitada pudiera tener eficacia jurídica el acuerdo de conciliación o de mediación que pudiera alcanzarse, aun estando exceptuado el proceso del referido requisito del intento previo, si las partes acuden en tiempo oportuno voluntariamente y de común acuerdo a tales vías previas, se suspenderán los plazos de caducidad o se interrumpirán los de prescripción en la forma establecida en el artículo siguiente.»

Dos. El artículo 69 queda redactado como sigue:

> **«Artículo 69.** *Agotamiento de la vía administrativa previa a la vía judicial social.*
>
> 1. Para poder demandar al Estado, Comunidades Autónomas, entidades locales o entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de los mismos será requisito necesario haber agotado la vía administrativa, cuando así proceda, de acuerdo con lo establecido en la normativa de procedimiento administrativo aplicable.
>
> En todo caso, la Administración pública deberá notificar a los interesados las resoluciones y actos administrativos que afecten a sus derechos e intereses,

conteniendo la notificación el texto íntegro de la resolución, con indicación de si es o no definitivo en la vía administrativa, la expresión de los recursos que procedan, órgano ante el que hubieran de presentarse y plazo para interponerlos, sin perjuicio de que los interesados puedan ejercitar, en su caso, cualquier otro que estimen procedente.

Las notificaciones que conteniendo el texto íntegro del acto omitiesen alguno de los demás requisitos previstos en el párrafo anterior mantendrán suspendidos los plazos de caducidad e interrumpidos los de prescripción y únicamente surtirán efecto a partir de la fecha en que el interesado realice actuaciones que supongan el conocimiento del contenido y alcance de la resolución o acto objeto de la notificación o resolución, o interponga cualquier recurso que proceda.

2. Desde que se deba entender agotada la vía administrativa el interesado podrá formalizar la demanda en el plazo de dos meses ante el juzgado o la Sala competente. A la demanda se acompañará copia de la resolución denegatoria o documento acreditativo de la interposición o resolución del recurso administrativo, según proceda, uniendo copia de todo ello para la entidad demandada.

3. En las acciones derivadas de despido y demás acciones sujetas a plazo de caducidad, el plazo de interposición de la demanda será de veinte días hábiles o el especial que sea aplicable, contados a partir del día siguiente a aquél en que se hubiera producido el acto o la notificación de la resolución impugnada, o desde que se deba entender agotada la vía administrativa en los demás casos.»

Tres. El artículo 70 queda redactado como sigue:

«Artículo 70. *Excepciones al agotamiento de la vía administrativa.*

No será necesario agotar la vía administrativa para interponer demanda de tutela de derechos fundamentales y libertades públicas frente a actos de las Administraciones públicas en el ejercicio de sus potestades en materia laboral y sindical, si bien el plazo para la interposición de la demanda será de veinte días desde el día siguiente a la notificación del acto o al transcurso del plazo fijado para la resolución, sin más trámites; cuando la lesión del derecho fundamental tuviera su origen en la inactividad administrativa o en actuación en vías de hecho, o se hubiera interpuesto potestativamente un recurso administrativo, el plazo de veinte días se iniciará transcurridos veinte días desde la reclamación contra la inactividad o vía de hecho, o desde la presentación del recurso, respectivamente.»

Cuatro. El artículo 72 queda redactado como sigue:

«Artículo 72. *Vinculación respecto a la reclamación administrativa previa en materia de prestaciones de Seguridad Social o vía administrativa previa.*

En el proceso no podrán introducir las partes variaciones sustanciales de tiempo, cantidades o conceptos respecto de los que fueran objeto del procedimiento administrativo y de las actuaciones de los interesados o de la Administración, bien en fase de reclamación previa en materia de prestaciones de Seguridad Social o de recurso que agote la vía administrativa, salvo en cuanto a los hechos nuevos o que no hubieran podido conocerse con anterioridad.»

Cinco. El artículo 73 queda redactado como sigue:

«Artículo 73. *Efectos de la reclamación administrativa previa en materia de prestaciones de Seguridad Social.*

La reclamación previa en materia de prestaciones de Seguridad Social interrumpirá los plazos de prescripción y suspenderá los de caducidad, reanudándose estos últimos al día siguiente al de la notificación de la resolución o del transcurso del plazo en que deba entenderse desestimada.»

Seis. El artículo 85 queda redactado como sigue:

«Artículo 85. *Celebración del juicio.*

1. Si no hubiera avenencia en conciliación, se pasará seguidamente a juicio y se dará cuenta de lo actuado.

Con carácter previo se resolverá, motivadamente, en forma oral y oídas las partes, sobre las cuestiones previas que se puedan formular en ese acto, así como sobre los recursos u otras incidencias pendientes de resolución, sin perjuicio de la ulterior sucinta fundamentación en la sentencia, cuando proceda. Igualmente serán oídas las partes y, en su caso, se resolverá, motivadamente y en forma oral, lo procedente sobre las cuestiones que el juez o tribunal pueda plantear en ese momento sobre su competencia, los presupuestos de la demanda o el alcance y límites de la pretensión formulada, respetando las garantías procesales de las partes y sin prejuzgar el fondo del asunto.

A continuación, el demandante ratificará o ampliará su demanda, aunque en ningún caso podrá hacer en ella variación sustancial.

2. El demandado contestará afirmando o negando concretamente los hechos de la demanda, y alegando cuantas excepciones estime procedentes.

3. Únicamente podrá formular reconvención cuando la hubiese anunciado en la conciliación previa al proceso o en la contestación a la reclamación previa en materia de prestaciones de Seguridad Social o resolución que agote la vía administrativa, y hubiese expresado en esencia los hechos en que se funda y la petición en que se concreta. No se admitirá la reconvención, si el órgano judicial no es competente, si la acción que se ejercita ha de ventilarse en modalidad procesal distinta y la acción no fuera acumulable, y cuando no exista conexión entre sus pretensiones y las que sean objeto de la demanda principal.

No será necesaria reconvención para alegar compensación de deudas, siempre que sean vencidas y exigibles y no se formule pretensión de condena reconvencional, y en general cuando el demandado esgrima una pretensión que tienda exclusivamente a ser absuelto de la pretensión o pretensiones objeto de la demanda principal, siendo suficiente que se alegue en la contestación a la demanda. Si la obligación precisa de determinación judicial por no ser líquida con antelación al juicio, será necesario expresar concretamente los hechos que fundamenten la excepción y la forma de liquidación de la deuda, así como haber anunciado la misma en la conciliación o mediación previas, o en la reclamación en materia de prestaciones de Seguridad Social o resolución que agoten la vía administrativa. Formulada la reconvención, se dará traslado a las demás partes para su contestación en los términos establecidos para la demanda. El mismo trámite de traslado se acordará para dar respuesta a las excepciones procesales, caso de ser alegadas.

4. Las partes harán uso de la palabra cuantas veces el juez o tribunal lo estime necesario.

5. Asimismo, en este acto, las partes podrán alegar cuanto estimen conveniente a efectos de lo dispuesto en la letra b) del apartado 3 del artículo 191, ofreciendo, para el momento procesal oportuno, los elementos de juicio necesarios para fundamentar sus alegaciones. No será preciso aportar prueba sobre esta concreta cuestión cuando el hecho de que el proceso afecta a muchos trabajadores o beneficiarios sea notorio por su propia naturaleza.

6. Si no se suscitasen cuestiones procesales o si, suscitadas, se hubieran contestado, las partes o sus defensores con el tribunal fijarán los hechos sobre los que exista conformidad o disconformidad de los litigantes, consignándose en caso necesario en el acta o, en su caso, por diligencia, sucinta referencia a aquellos extremos esenciales conformes, a efectos de ulterior recurso. Igualmente podrán facilitar las partes unas notas breves de cálculo o resumen de datos numéricos.

7. En caso de allanamiento total o parcial será aprobado por el órgano jurisdiccional, oídas las demás partes, de no incurrir en renuncia prohibida de derechos, fraude de ley o perjuicio a terceros, o ser contrario al interés público, mediante resolución que podrá dictarse en forma oral. Si el allanamiento fuese total se dictará sentencia condenatoria de acuerdo con las pretensiones del actor. Cuando

el allanamiento sea parcial, podrá dictarse auto aprobatorio, que podrá llevarse a efecto por los trámites de la ejecución definitiva parcial, siempre que por la naturaleza de las pretensiones objeto de allanamiento, sea posible un pronunciamiento separado que no prejuzgue las restantes cuestiones no allanadas, respecto de las cuales continuará el acto de juicio.

8. El juez o tribunal, una vez practicada la prueba y antes de las conclusiones, salvo que exista oposición de alguna de las partes, podrá suscitar la posibilidad de llegar a un acuerdo y de no alcanzarse el mismo en ese momento proseguirá la celebración del juicio.»

Siete. El artículo 103 queda redactado como sigue:

«Artículo 103. *Presentación de la demanda por despido.*

1. El trabajador podrá reclamar contra el despido, dentro de los veinte días hábiles siguientes a aquél en que se hubiera producido. Dicho plazo será de caducidad a todos los efectos y no se computarán los sábados, domingos y los festivos en la sede del órgano jurisdiccional.

2. Si se promoviese papeleta de conciliación o solicitud de mediación o demanda por despido contra una persona a la que erróneamente se hubiere atribuido la cualidad de empresario, y se acreditase con posterioridad, sea en el juicio o en otro momento anterior del proceso, que lo era un tercero, el trabajador podrá promover nueva demanda contra éste, o ampliar la demanda si no se hubiera celebrado el juicio, sin que comience el cómputo del plazo de caducidad hasta el momento en que conste quién sea el empresario.

3. Las normas del presente capítulo serán de aplicación a la impugnación de las decisiones empresariales de extinción de contrato con las especialidades necesarias, sin perjuicio de lo previsto en el artículo 120 y de las consecuencias sustantivas de cada tipo de extinción contractual.»

Ocho. El artículo 117 queda redactado como sigue:

«Artículo 117. *Requisito del agotamiento de la vía administrativa previa a la vía judicial.*

1. Para demandar al Estado por los salarios de tramitación, será requisito previo haber reclamado en vía administrativa en la forma y plazos establecidos, contra cuya denegación el empresario o, en su caso, el trabajador, podrá promover la oportuna acción ante el juzgado que conoció en la instancia del proceso de despido.

2. A la demanda habrá de acompañarse copia de la resolución administrativa denegatoria o de la instancia de solicitud de pago.

3. El plazo de prescripción de esta acción es el previsto en el apartado 2 del artículo 59 del texto refundido de la Ley del Estatuto de los Trabajadores, iniciándose el cómputo del mismo, en caso de reclamación efectuada por el empresario, desde el momento en que éste sufre la disminución patrimonial ocasionada por el abono de los salarios de tramitación y, en caso de reclamación por el trabajador, desde la fecha de notificación al mismo del auto judicial que haya declarado la insolvencia del empresario.»

Disposición final cuarta. *Referencias normativas.*

Las referencias hechas a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, se entenderán hechas a la Ley del Procedimiento Administrativo Común de las Administraciones Públicas o a la Ley de Régimen Jurídico del Sector Público, según corresponda.

Disposición final quinta. *Adaptación normativa.*

En el plazo de un año a partir de la entrada en vigor de la Ley, se deberán adecuar a la misma las normas reguladoras estatales, autonómicas y locales de los distintos procedimientos normativos que sean incompatibles con lo previsto en esta Ley.

Disposición final sexta. *Desarrollo normativo de la Ley.*

Se faculta al Consejo de Ministros y al Ministro de Hacienda y Administraciones Públicas, en el ámbito de sus competencias, para dictar cuantas disposiciones reglamentarias sean necesarias para el desarrollo de la presente Ley, así como para acordar las medidas necesarias para garantizar la efectiva ejecución e implantación de las previsiones de esta Ley.

Disposición final séptima. *Entrada en vigor.*

La presente Ley entrará en vigor al año de su publicación en el “Boletín Oficial del Estado”.

No obstante, las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico producirán efectos a partir del día 2 de abril de 2021.

§ 3

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

Jefatura del Estado
«BOE» núm. 236, de 2 de octubre de 2015
Última modificación: 24 de diciembre de 2022
Referencia: BOE-A-2015-10566

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

El 26 de octubre de 2012 el Consejo de Ministros acordó la creación de la Comisión para la Reforma de las Administraciones Públicas con el mandato de realizar un estudio integral dirigido a modernizar el sector público español, dotarle de una mayor eficacia y eliminar las duplicidades que le afectaban y simplificar los procedimientos a través de los cuales los ciudadanos y las empresas se relacionan con la Administración.

El informe, que fue elevado al Consejo de Ministros el 21 de junio de 2013, formuló 218 propuestas basadas en el convencimiento de que una economía competitiva exige unas Administraciones Públicas eficientes, transparentes, ágiles y centradas en el servicio a los ciudadanos y las empresas. En la misma línea, el Programa nacional de reformas de España para 2014 establece la necesidad de impulsar medidas para racionalizar la actuación administrativa, mejorar la eficiencia en el uso de los recursos públicos y aumentar su productividad.

Este convencimiento está inspirado en lo que dispone el propio artículo 31.2 de la Constitución Española, cuando establece que el gasto público realizará una asignación equitativa de los recursos públicos, y su programación y ejecución responderán a los criterios de eficiencia y economía.

Como se señala en el Informe de la Comisión para la Reforma de las Administraciones Públicas (en adelante CORA), la normativa reguladora de las Administraciones Públicas ha pasado por diferentes etapas. Tradicionalmente, las reglas reguladoras de los aspectos orgánicos del poder ejecutivo estaban separadas de las que disciplinaban los procedimientos. Esta separación terminó con la Ley 30/1992, de 26 de noviembre, de

Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, que unificó en un solo instrumento estas materias.

La evolución normativa posterior se ha caracterizado por la profusión de leyes, reales decretos y demás disposiciones de inferior rango, que han completado la columna vertebral del derecho administrativo. De este modo, nos encontramos en el momento actual normas que regulan aspectos orgánicos, como la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado; la Ley 50/1997, de 27 de noviembre, del Gobierno y la Ley 28/2006, de 18 de julio, de Agencias estatales para la mejora de los servicios públicos; y otras que tratan aspectos tanto orgánicos como procedimentales de la citada Ley 30/1992, de 26 de noviembre; o la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, por citar las más relevantes.

Resulta, por tanto evidente, la necesidad de dotar a nuestro sistema legal de un derecho administrativo sistemático, coherente y ordenado, de acuerdo con el proyecto general de mejora de la calidad normativa que inspira todo el informe aprobado por la CORA. En él se previó la elaboración de dos leyes: una, reguladora del procedimiento administrativo, que integraría las normas que rigen la relación de los ciudadanos con las Administraciones. Otra, comprensiva del régimen jurídico de las Administraciones Públicas, donde se incluirían las disposiciones que disciplinan el sector público institucional. Con ello, se aborda una reforma integral de la organización y funcionamiento de las Administraciones articulada en dos ejes fundamentales: la ordenación de las relaciones ad extra de las Administraciones con los ciudadanos y empresas, y la regulación ad intra del funcionamiento interno de cada Administración y de las relaciones entre ellas.

La presente Ley responde al segundo de los ejes citados, y abarca, por un lado, la legislación básica sobre régimen jurídico administrativo, aplicable a todas las Administraciones Públicas; y por otro, el régimen jurídico específico de la Administración General del Estado, donde se incluye tanto la llamada Administración institucional, como la Administración periférica del Estado. Esta Ley contiene también la regulación sistemática de las relaciones internas entre las Administraciones, estableciendo los principios generales de actuación y las técnicas de relación entre los distintos sujetos públicos. Queda así sistematizado el ordenamiento de las relaciones ad intra e inter Administraciones, que se complementa con su normativa presupuestaria, destacando especialmente la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, la Ley 47/2003, de 26 de noviembre, General Presupuestaria y las leyes anuales de Presupuestos Generales del Estado.

Se conserva como texto independiente la Ley del Gobierno, que por regular de forma específica la cabeza del poder ejecutivo de la nación, de naturaleza y funciones eminentemente políticas, debe mantenerse separada de la norma reguladora de la Administración Pública, dirigida por aquél. De acuerdo con este criterio, la presente Ley modifica aquella, con el objeto de extraer aquellas materias que, por ser más propias de la organización y funciones de los miembros del gobierno en cuanto que órganos administrativos, deben regularse en este texto legal.

El Informe CORA recomienda reformar el ordenamiento jurídico administrativo no solo por razones de coherencia normativa y política legislativa. Las Administraciones Públicas, lejos de constituir un obstáculo para la vida de los ciudadanos y las empresas, deben facilitar la libertad individual y el desenvolvimiento de la iniciativa personal y empresarial. Para ello es imprescindible establecer un marco normativo que impida la creación de órganos o entidades innecesarios o redundantes, y asegure la eficacia y eficiencia de los entes públicos, ejerciendo sobre ellos una supervisión continua que permita evaluar el cumplimiento de los objetivos que justificaron su creación, y cuestionar su mantenimiento cuando aquellos se hayan agotado o exista otra forma más eficiente de alcanzarlos.

La Organización para la Cooperación y Desarrollo Económico (en adelante OCDE), ha valorado la reforma administrativa emprendida por la CORA de forma muy positiva. En el informe emitido sobre ella, señala que el paquete de reforma es resultado de un riguroso proceso de recolección de datos, diálogo entre profesionales y diagnóstico de las debilidades de la Administraciones Públicas españolas. Considera la OCDE que el conjunto de asuntos políticos incluidos en la reforma (por ejemplo, gobierno electrónico, relaciones de

gobernanza multinivel, buena regulación, reformas presupuestarias), junto con las iniciativas paralelas adoptadas en los dos últimos años en áreas como estabilidad presupuestaria, transparencia y regeneración democrática, explica uno de los más ambiciosos procesos de reforma realizados en un país de la OCDE. La presente Ley, por tanto, no representa el único instrumento normativo que materializa la reforma, Pero sí constituye, junto con la que disciplinará el procedimiento administrativo, de tramitación paralela, y las ya aprobadas sobre transparencia y buen gobierno y estabilidad presupuestaria, la piedra angular sobre la que se edificará la Administración Pública española del futuro, al servicio de los ciudadanos.

II

La Ley comienza estableciendo, en sus disposiciones generales, los principios de actuación y de funcionamiento del sector público español.

Entre los principios generales, que deberán respetar todas las Administraciones Públicas en su actuación y en sus relaciones recíprocas, además de encontrarse los ya mencionados en la Constitución Española de eficacia, jerarquía, descentralización, desconcentración, coordinación, y sometimiento pleno a la Ley y al Derecho, destaca la incorporación de los de trasparencia y de planificación y dirección por objetivos, como exponentes de los nuevos criterios que han de guiar la actuación de todas las unidades administrativas.

La Ley recoge, con las adaptaciones necesarias, las normas hasta ahora contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del sector público, y algunas de las previstas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la anterior. Se integran así materias que demandaban una regulación unitaria, como corresponde con un entorno en el que la utilización de los medios electrónicos ha de ser lo habitual, como la firma y sedes electrónicas, el intercambio electrónico de datos en entornos cerrados de comunicación y la actuación administrativa automatizada. Se establece asimismo la obligación de que las Administraciones Públicas se relacionen entre sí por medios electrónicos, previsión que se desarrolla posteriormente en el título referente a la cooperación interadministrativa mediante una regulación específica de las relaciones electrónicas entre las Administraciones. Para ello, también se contempla como nuevo principio de actuación la interoperabilidad de los medios electrónicos y sistemas y la prestación conjunta de servicios a los ciudadanos.

La enumeración de los principios de funcionamiento y actuación de las Administraciones Públicas se completa con los ya contemplados en la normativa vigente de responsabilidad, calidad, seguridad, accesibilidad, proporcionalidad, neutralidad y servicio a los ciudadanos.

El Título Preliminar regula pormenorizadamente el régimen de los órganos administrativos, tomando como base la normativa hasta ahora vigente contenida en la Ley 30/1992, de 26 de noviembre, en la que se incorporan ciertas novedades. La creación de órganos solo podrá hacerse previa comprobación de que no exista ninguna duplicidad con los existentes. Se completan las previsiones sobre los órganos de la Administración consultiva y se mejora la regulación de los órganos colegiados, en particular, los de la Administración General del Estado, destacando la generalización del uso de medios electrónicos para que éstos puedan constituirse, celebrar sus sesiones, adoptar acuerdos, elaborar y remitir las actas de sus reuniones.

También se incorporan en este Título los principios relativos al ejercicio de la potestad sancionadora y los que rigen la responsabilidad patrimonial de las Administraciones Públicas. Entre las novedades más destacables en este ámbito, merecen especial mención los cambios introducidos en la regulación de la denominada «responsabilidad patrimonial del Estado Legislador» por las lesiones que sufran los particulares en sus bienes y derechos derivadas de leyes declaradas inconstitucionales o contrarias al Derecho de la Unión Europea, concretándose las condiciones que deben darse para que se pueda proceder, en su caso, a la indemnización que corresponda.

Por último, se regulan en el Título Preliminar los convenios administrativos, en la línea prevista en el Dictamen 878 del Tribunal de Cuentas, de 30 de noviembre, de 2010, que recomendaba sistematizar su marco legal y tipología, establecer los requisitos para su validez, e imponer la obligación de remitirlos al propio Tribunal. De este modo, se desarrolla un régimen completo de los convenios, que fija su contenido mínimo, clases, duración, y extinción y asegura su control por el Tribunal de Cuentas.

III

En relación con la Administración del Estado, el Título primero parte de la regulación contenida en la Ley 6/1997, de 14 de abril, aplicando ciertas mejoras que el tiempo ha revelado necesarias. Se establecen los órganos superiores y directivos propios de la estructura ministerial y también en el ámbito de la Administración periférica y en el exterior. En el caso de los organismos públicos, serán sus estatutos los que establezcan sus órganos directivos.

La Ley regula los Ministerios y su organización interna, sobre la base de los siguientes órganos: Ministros, Secretarios de Estado, Subsecretarios, Secretarios Generales, Secretarios Generales Técnicos, Directores Generales y Subdirectores Generales.

Se integran en esta Ley funciones de los Ministros que, hasta ahora, estaban dispersas en otras normas o que eran inherentes al ejercicio de ciertas funciones, como celebrar en el ámbito de su competencia, contratos y convenios; autorizar las modificaciones presupuestarias; decidir la representación del Ministerio en los órganos colegiados o grupos de trabajo; rendir la cuenta del departamento ante el Tribunal de Cuentas; y resolver los recursos administrativos presentados ante los órganos superiores y directivos del Departamento. La Ley reordena parcialmente las competencias entre los órganos superiores, Ministros y Secretarios de Estado, y directivos, Subsecretarios, Secretarios Generales, Secretarios Generales Técnicos y Directores Generales de los Ministerios, atribuyendo a ciertos órganos como propias algunas funciones que hasta ahora habitualmente se delegaban en ellos. Y con el objeto de posibilitar las medidas de mejora de gestión propuestas en el Informe CORA, se atribuye a los Subsecretarios una nueva competencia: la de adoptar e impulsar las medidas tendentes a la gestión centralizada de recursos y medios materiales en el ámbito de su Departamento.

Se atribuyen también expresamente a la Subsecretaría del Ministerio de la Presidencia, en coordinación con la Secretaría General de la Presidencia del Gobierno, las competencias propias de los servicios comunes de los Departamentos en relación con el área de la Presidencia del Gobierno. Debe recordarse que, al tratarse de un ámbito ajeno a la estructura del propio departamento ministerial, esta atribución excede del real decreto en que se fije la estructura orgánica de aquél.

Con el objeto de evitar la proliferación de centros encargados de la prestación de servicios administrativos en cada ente o unidad, y facilitar que los mismos se provean por órganos especializados en el ámbito del Ministerio o de forma centralizada para toda la Administración, se prevé la posibilidad de que la organización y gestión de los servicios comunes de los Ministerios y entidades dependientes pueda ser coordinada por el Ministerio de Hacienda y Administraciones Públicas u otro organismo público; o bien por la Subsecretaría de cada departamento.

IV

Sobre la base de la regulación de la Administración Periférica contenida en la Ley 6/1997, la Ley regula los órganos de la Administración General del Estado de carácter territorial, los Delegados y Subdelegados del Gobierno. Como principales novedades respecto a la regulación hasta ahora vigente, destacan las siguientes cuestiones.

En cuanto a los Delegados del Gobierno, se refuerza su papel político e institucional, se les define como órganos directivos, y se dispone que su nombramiento atenderá a criterios de competencia profesional y experiencia, siendo de aplicación al desempeño de sus funciones lo establecido en el Título II de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Se mejora la regulación de su suplencia, vacante o enfermedad, correspondiendo al Subdelegado del Gobierno que el Delegado designe. En caso de no haber realizado formalmente la designación, y cuando se trate de una Comunidad uniprovincial que carezca de Subdelegado, la suplencia recaerá sobre el Secretario General.

Las competencias de los Delegados del Gobierno, que hasta ahora eran recogidas en diversos preceptos, pasan a estar reguladas en un único artículo, sistematizándolas en cinco categorías: competencias de dirección y coordinación; de información de la acción del Gobierno y a los ciudadanos; de coordinación y colaboración con otras Administraciones

Públicas; competencias relativas al control de legalidad; y competencias relacionadas con el desarrollo de las políticas públicas.

Se recoge expresamente en la Ley la competencia atribuida a los Delegados del Gobierno en la Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones Públicas, referente a la coordinación de los usos de los edificios de la Administración General del Estado en su ámbito de actuación, de acuerdo con las directrices establecidas por el Ministerio de Hacienda y Administraciones Públicas y la Dirección General de Patrimonio del Estado.

Respecto de los Subdelegados del Gobierno, se concretan los requisitos de titulación para ser nombrado Subdelegado del Gobierno, de tal manera que ahora se indica el subgrupo funcionarial al que debe pertenecer. En cuanto a las competencias de los Subdelegados del Gobierno, y como novedad más relevante, se le atribuye la de coordinar la utilización de los medios materiales y, en particular, de los edificios administrativos en el ámbito de su provincia.

Se recoge legalmente la existencia de un órgano que se ha revelado como fundamental en la gestión de las Delegaciones y Subdelegaciones, la Secretaría General, encargada de la llevanza de los servicios comunes y de la que dependerán las áreas funcionales. También se establece a nivel legal que la asistencia jurídica y el control financiero de las Delegaciones y Subdelegaciones del Gobierno serán ejercidos por la Abogacía del Estado y por la Intervención General de la Administración del Estado, respectivamente, cuestión anteriormente regulada por normativa reglamentaria.

La Ley también prevé expresamente la existencia de la Comisión Interministerial de Coordinación de la Administración Periférica del Estado, cuyas atribuciones, composición y funcionamiento serán objeto de regulación reglamentaria.

Por lo que se refiere a la Administración General del Estado en el exterior, se efectúa una remisión a la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, y a su normativa de desarrollo, declarándose la aplicación supletoria de la presente Ley.

V

En el ámbito de la denominada Administración institucional, la Ley culmina y hace efectivas las conclusiones alcanzadas en este ámbito por la CORA y que son reflejo de la necesidad de dar cumplimiento a lo previsto en el mencionado artículo 31.2 de la Constitución, que ordena que el gasto público realice una asignación equitativa de los recursos públicos, y que su programación y ejecución respondan a los criterios de eficiencia y economía. De forma congruente con este mandato, el artículo 135 de la Constitución establece que todas las Administraciones Públicas adecuarán sus actuaciones al principio de estabilidad presupuestaria.

La permanente necesidad de adaptación de la Administración Institucional se aprecia con el mero análisis de la regulación jurídica de los entes que la componen. Un panorama en el que se han aprobado de forma sucesiva diferentes leyes que desde distintas perspectivas han diseñado el marco normativo de los entes auxiliares de que el Estado dispone.

En primer lugar, la regulación jurídica fundamental de los diferentes tipos de entes y organismos públicos dependientes del Estado está prevista en la Ley 6/1997, de 14 de abril, que diferencia tres tipos de entidades: Organismos Autónomos, Entidades Públicas Empresariales y Agencias Estatales, categoría que se añadió con posterioridad. Cada uno de estos organismos públicos cuenta con una normativa reguladora específica, que normalmente consta de una referencia en la ley de creación y de un desarrollo reglamentario posterior dictado al aprobar los correspondientes estatutos.

No obstante, el marco aparentemente general es cuestionado por la previsión establecida en la disposición adicional décima de la Ley, 6/1997, de 14 de abril, que excluye de su aplicación a determinados entes que cuentan con previsiones legales propias, por lo que la Ley se les aplica de forma sólo supletoria. Esta excepción pone de relieve el principal obstáculo en la clarificación normativa de estos entes, que no es otro que el desplazamiento del derecho común en beneficio de un derecho especial normalmente vinculado a una percepción propia de un sector de actividad, social o corporativo, que a través de la legislación específica logra dotarse de un marco jurídico más sensible a sus necesidades.

Con posterioridad a la Ley 6/1997, de 14 de abril, la descentralización funcional del Estado recuperó rápidamente su tendencia a la diversidad. En primer lugar, por la aprobación de la Ley 50/2002, de 26 de diciembre, de Fundaciones. En ella se diseña el régimen aplicable a las fundaciones constituidas mayoritariamente por entidades del sector público estatal, aplicando la técnica fundacional al ámbito de la gestión pública.

Desde otra perspectiva, basada en el análisis de la actividad que realizan los diferentes entes, el ordenamiento vigente ha regulado en la Ley 47/2003, de 26 de noviembre, General Presupuestaria, la totalidad del denominado «sector público estatal», que está formado por tres sectores: Primero, el Sector Público administrativo, que está constituido por la Administración General del Estado; los organismos autónomos dependientes de la Administración General del Estado; las entidades gestoras, servicios comunes y las mutuas colaboradoras con la Seguridad Social en su función pública de colaboración en la gestión de la Seguridad Social; los órganos con dotación diferenciada en los Presupuestos Generales del Estado que, careciendo de personalidad jurídica, no están integrados en la Administración General del Estado pero forman parte del sector público estatal; las entidades estatales de derecho público y los consorcios, cuando sus actos estén sujetos directa o indirectamente al poder de decisión de un órgano del Estado, su actividad principal no consista en la producción en régimen de mercado de bienes y servicios y no se financien mayoritariamente con ingresos comerciales. Segundo, el Sector Público empresarial, que está constituido por las entidades públicas empresariales, dependientes de la Administración General del Estado, o de cualesquiera otros organismos públicos vinculados o dependientes de ella; las sociedades mercantiles estatales, definidas en la Ley 33/2003, de 3 de noviembre, de Patrimonio de las Administraciones Públicas; y las Entidades estatales de derecho público distintas de las comprendidas en el Sector Público administrativo y los consorcios no incluidos en él. Tercero, el Sector Público fundacional, constituido por las fundaciones del sector público estatal, definidas en la Ley 50/2002, de 26 de diciembre.

El siguiente hito normativo fue la Ley 33/2003, de 3 de noviembre, que regula el denominado «patrimonio empresarial de la Administración General del Estado», formado por las entidades públicas empresariales, a las que se refiere el Capítulo III del Título III de la Ley 6/1997, de 14 de abril, las entidades de Derecho público cuyos ingresos provengan, al menos en un 50 por 100, de operaciones realizadas en el mercado; y las sociedades mercantiles estatales.

La preocupación por la idoneidad de los entes públicos y la voluntad de abordar su reforma condujo a la aprobación de la Ley 28/2006, de 18 de julio, de Agencias Estatales para la Mejora de los Servicios Públicos, mediante la que se creó este nuevo tipo de ente. El objetivo prioritario de esta Ley fue establecer mecanismos de responsabilidad en la dirección y gestión de los nuevos organismos públicos, vinculando el sistema retributivo al logro de sus objetivos y reconociendo un mayor margen de discrecionalidad en la gestión presupuestaria.

La Ley autorizó la creación de 12 Agencias, si bien hasta el momento sólo se han constituido 7 de ellas, y la Agencia Española de Medicamentos y Productos Sanitarios, autorizada en otra Ley.

El objetivo de la reforma fue instaurar la Agencia como nuevo modelo de ente público, pero nació ya con una eficacia limitada. La disposición adicional quinta de la Ley autorizaba al Gobierno para transformar en Agencia los Organismos Públicos cuyos objetivos y actividades se ajustasen a su naturaleza, lo que implicaba el reconocimiento de la existencia de entidades que, por no cumplir este requisito, no precisarían transformación, y que permanecerían en su condición de Organismos Autónomos, Entidades Públicas Empresariales o entes con estatuto especial. Y, sin embargo, la disposición adicional séptima ordenaba atribuir el estatuto a todos los organismos públicos de futura creación «con carácter general».

Por todo ello, no puede decirse que los objetivos de la Ley se hayan alcanzado, incluso después de más de seis años de vigencia, porque su desarrollo posterior ha sido muy limitado, y porque las medidas de control de gasto público han neutralizado la pretensión de dotar a las agencias de mayor autonomía financiera.

Otras normas se han referido con mayor o menor amplitud, al ámbito y categoría del sector público. Es el caso de la Ley 30/2007, de 30 de octubre, de Contratos del Sector

Público, que diferencia entre el «Sector Público» y las «Administraciones Públicas», introduciendo el concepto de «poderes adjudicadores». Distinción igualmente recogida en el posterior Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

La Ley 2/2011, de 4 de marzo, de Economía Sostenible, llevó a cabo una regulación propia y especial para los seis organismos reguladores existentes en esos momentos, con especial atención a garantizar su independencia respecto de los agentes del mercado. Posteriormente la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia integró en esta supervisión hasta siete preexistentes. Incluso nos encontramos con que la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, para evitar dudas interpretativas, se remite a la definición del «sector público» «en el ámbito comunitario».

El proyecto de reforma administrativa puesto en marcha aborda la situación de los entes instrumentales en dos direcciones: medidas concretas de racionalización del sector público estatal, fundacional y empresarial, que se han materializado en sucesivos Acuerdos de Consejo de Ministros, y en otras disposiciones; y la reforma del ordenamiento aplicable a los mismos, que se materializa en la presente Ley, y de la que ya se habían dado pasos en la reciente Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa, que modificó el régimen jurídico de los consorcios.

Teniendo en cuenta todos estos antecedentes, la Ley establece, en primer lugar, dos normas básicas para todas las Administraciones Públicas. Por un lado, la obligatoriedad de inscribir la creación, transformación o extinción de cualquier entidad integrante del sector público institucional en el nuevo Inventario de Entidades del Sector Público Estatal, Autonómico y Local. Esta inscripción será requisito necesario para obtener el número de identificación fiscal definitivo de la Agencia Estatal de Administración Tributaria. Este Registro permitirá contar con información completa, fiable y pública del número y los tipos de organismos públicos y entidades existentes en cada momento. Y por otro lado, se obliga a todas las Administraciones a disponer de un sistema de supervisión continua de sus entidades dependientes, que conlleve la formulación periódica de propuestas de transformación, mantenimiento o extinción.

Ya en el ámbito de la Administración General del Estado, se establece una nueva clasificación del sector público estatal para los organismos y entidades que se creen a partir de la entrada en vigor de la Ley, más clara, ordenada y simple, pues quedan reducidos a los siguientes tipos: organismos públicos, que incluyen los organismos autónomos y las entidades públicas empresariales; autoridades administrativas independientes, sociedades mercantiles estatales, consorcios, fundaciones del sector público y fondos sin personalidad jurídica. La meta es la de sistematizar el régimen hasta ahora vigente en el ámbito estatal y mejorarlo siguiendo las pautas que se explican a continuación.

En primer lugar, preservando los aspectos positivos de la regulación de los distintos tipos de entes, de modo que se favorezca la programación de objetivos, el control de eficacia de los entes públicos y el mantenimiento de los estrictamente necesarios para la realización de las funciones legalmente encomendadas al sector público.

En segundo lugar, suprimiendo las especialidades que, sin mucha justificación, propiciaban la excepción de la aplicación de controles administrativos que deben existir en toda actuación pública, en lo que ha venido en denominarse la «huida del derecho administrativo». La flexibilidad en la gestión ha de ser compatible con los mecanismos de control de la gestión de fondos públicos.

Y, en tercer lugar, dedicando suficiente atención a la supervisión de los entes públicos y a su transformación y extinción, materias éstas que, por poco frecuentes, no habían demandado un régimen detallado en el pasado. Con ello se resuelve una de las principales carencias de la Ley de Agencias: la ausencia de una verdadera evaluación externa a la entidad, que permita juzgar si sigue siendo la forma más eficiente y eficaz posible de cumplir los objetivos que persiguió su creación y que proponga alternativas en caso de que no sea así.

De este modo, se establecen dos tipos de controles de las entidades integrantes del sector público estatal.

Una supervisión continua, desde su creación hasta su extinción, a cargo del Ministerio de Hacienda y Administraciones Públicas que vigilará la concurrencia de los requisitos previstos en esta Ley.

Un control de eficacia, centrado en el cumplimiento de los objetivos propios de la actividad de la entidad, que será ejercido anualmente por el Departamento al que esté adscrita la entidad u organismo público, sin perjuicio del control de la gestión económico financiera que se ejerza por la Intervención General de la Administración del Estado.

Este sistema, que sigue las mejores prácticas del derecho comparado, permitirá evaluar de forma continua la pervivencia de las razones que justificaron la creación de cada entidad y su sostenibilidad futura. Así se evitará tener que reiterar en el futuro el exhaustivo análisis que tuvo que ejecutar la CORA para identificar las entidades innecesarias o redundantes y que están en proceso de extinción.

Se incorpora al contenido de la Ley la regulación de los medios propios y servicios técnicos de la Administración, de acuerdo con lo que en la actualidad se establece en la normativa de contratos del sector público. Como novedad, la creación de un medio propio o su declaración como tal deberá ir precedida de una justificación, por medio de una memoria de la intervención general, de que la entidad resulta sostenible y eficaz, de acuerdo con los criterios de rentabilidad económica, y que resulta una opción más eficiente que la contratación pública para disponer del servicio o suministro cuya provisión le corresponda, o que concurren otras razones excepcionales que justifican su existencia, como la seguridad pública o la urgencia en la necesidad del servicio. Asimismo, estas entidades deberán estar identificadas a través de un acrónimo «MP», para mayor seguridad jurídica. Estos requisitos se aplicarán tanto a los medios propios que se creen en el futuro como a los ya existentes, estableciéndose un plazo de seis meses para su adaptación.

Bajo la denominación de «organismos públicos», la Ley regula los organismos autónomos y las entidades públicas empresariales del sector público estatal.

Los organismos públicos se definen como aquéllos dependientes o vinculados a la Administración General del Estado, bien directamente, bien a través de otro organismo público, cuyas características justifican su organización en régimen de descentralización funcional o de independencia, y que son creados para la realización de actividades administrativas, sean de fomento, prestación, gestión de servicios públicos o producción de bienes de interés público susceptibles de contraprestación, así como actividades de contenido económico reservadas a las Administraciones Públicas. Tienen personalidad jurídica pública diferenciada, patrimonio y tesorería propios, así como autonomía de gestión y les corresponden las potestades administrativas precisas para el cumplimiento de sus fines salvo la potestad expropiatoria.

Se establece una estructura organizativa común en el ámbito del sector público estatal, articulada en órganos de gobierno, ejecutivos y de control de eficacia, correspondiendo al Ministro de Hacienda y Administraciones Públicas la clasificación de las entidades, conforme a su naturaleza y a los criterios previstos en el Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos en el sector público empresarial y otras entidades.

En general, se hace más exigente la creación de organismos públicos al someterse a los siguientes requisitos: por un lado, la elaboración de un plan de actuación con un contenido mínimo que incluye un análisis de eficiencia y las razones que fundamentan la creación; justificación de la forma jurídica propuesta; determinación de los objetivos a cumplir y los indicadores para medirlos; acreditación de la inexistencia de duplicidades, etc. Y, por otro lado, un informe preceptivo del Ministerio de Hacienda y Administraciones Públicas.

De acuerdo con el criterio de racionalización anteriormente expuesto para toda la Administración General del Estado, tanto los organismos existentes en el sector público estatal como los de nueva creación aplicarán una gestión compartida de los servicios comunes, salvo que la decisión de no hacerlo se justifique en la memoria que acompañe a la norma de creación por razones de eficiencia, conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, seguridad nacional o cuando la organización y gestión compartida afecte a servicios que deban prestarse de forma autónoma en atención a la independencia del organismo.

Por primera vez, se incluye para el sector público estatal un régimen de transformaciones y fusiones de organismos públicos de la misma naturaleza jurídica, bien mediante su extinción e integración en un nuevo organismo público, o bien mediante su absorción por otro ya existente. La fusión se llevará a cabo por una norma reglamentaria, aunque suponga modificación de la ley de creación. Se establece un mayor control para la transformación de organismo autónomo en sociedad mercantil estatal o en fundación del sector público, con el fin de evitar el fenómeno de la huida de los controles del derecho administrativo, para lo que se exige la elaboración de una memoria que lo justifique y un informe preceptivo de la Intervención General de la Administración del Estado. En cambio, se facilita la transformación de sociedades mercantiles estatales en organismos autónomos, que están sometidos a controles más intensos.

Se regula, también en el ámbito estatal, la disolución, liquidación y extinción de organismos públicos. En este sentido, se detallan las causas de disolución, entre las que destaca la situación de desequilibrio financiero durante dos ejercicios presupuestarios consecutivos, circunstancia que no opera de modo automático, al poder corregirse mediante un plan elaborado al efecto.

El proceso de disolución es ágil, al bastar un acuerdo del Consejo de Ministros. Deberá designarse un órgano administrativo o entidad del sector público institucional como liquidador, cuya responsabilidad será directamente asumida por la Administración que le designe, sin perjuicio de la posibilidad de repetir contra aquél cuando hubiera causa legal para ello.

Publicado el acuerdo de disolución, la liquidación se inicia automáticamente, y tendrá lugar por cesión e integración global de todo el activo y pasivo del organismo en la Administración General del Estado, que sucederá a la entidad extinguida en todos sus derechos y obligaciones. Formalizada la liquidación se producirá la extinción automática.

En cuanto a la tipología propia del sector institucional del Estado, la Ley contempla las siguientes categorías de entidades: organismos públicos, que comprende los organismos autónomos y las entidades públicas empresariales; las autoridades administrativas independientes; las sociedades mercantiles estatales; las fundaciones del sector público estatal; los consorcios; y los fondos sin personalidad jurídica. En los capítulos correspondientes a cada tipo se define su régimen jurídico, económico-financiero, presupuestario, de contratación, y de personal. Los organismos autónomos desarrollan actividades derivadas de la propia Administración Pública, en calidad de organizaciones instrumentales diferenciadas y dependientes de ésta, mientras que las entidades públicas empresariales, se cualifican por simultanear el ejercicio de potestades administrativas y de actividades prestacionales, de gestión de servicios o de producción de bienes de interés público, susceptibles de contraprestación. Las autoridades administrativas independientes, tienen atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad económica, para cuyo desempeño deben estar dotadas de independencia funcional o una especial autonomía respecto de la Administración General del Estado, lo que deberá determinarse en una norma con rango de Ley. En atención a esta peculiar idiosincrasia, se rigen en primer término por su normativa especial, y supletoriamente, en cuanto sea compatible con su naturaleza y funciones, por la presente Ley.

Se mantiene el concepto de sociedades mercantiles estatales actualmente vigente en la Ley 33/2003, de 3 de noviembre, respecto de las cuales se incluye como novedad que la responsabilidad aplicable a los miembros de sus consejos de administración designados por la Administración General del Estado será asumida directamente por la Administración designante. Todo ello, sin perjuicio de que pueda exigirse de oficio la responsabilidad del administrador por los daños y perjuicios causados cuando hubiera concurrido dolo, o culpa o negligencia graves.

La Ley establece con carácter básico el régimen jurídico de los consorcios, al tratarse de un régimen que, por definición, afectará a todas las Administraciones Públicas, siguiendo la línea de las modificaciones efectuadas por la Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa. La creación de un consorcio en el que participe la Administración General del Estado ha de estar prevista en una ley e ir precedida de la autorización del Consejo de Ministros. El consorcio se constituye

mediante el correspondiente convenio, al que habrán de acompañarse los estatutos, un plan de actuación de igual contenido que el de los organismos públicos y el informe preceptivo favorable del departamento competente en la Hacienda Pública o la intervención general que corresponda. Las entidades consorciadas podrán acordar, con la mayoría que se establezca en los estatutos, o a falta de previsión estatutaria, por unanimidad, la cesión global de activos y pasivos a otra entidad jurídicamente adecuada con la finalidad de mantener la continuidad de la actividad y alcanzar los objetivos del consorcio que se liquida. Su disolución es automática mediante acuerdo del máximo órgano de gobierno del consorcio, que nombrará a un órgano o entidad como liquidador. La responsabilidad del empleado público que sea nombrado liquidador será asumida por la entidad o la Administración que lo designó, sin perjuicio de las acciones que esta pueda ejercer para, en su caso, repetir la responsabilidad que corresponda. Finalmente, cabe destacar que se avanza en el rigor presupuestario de los consorcios que estarán sujetos al régimen de presupuestación, contabilidad y control de la Administración Pública a la que estén adscritos y por tanto se integrarán o, en su caso, acompañarán a los presupuestos de la Administración de adscripción en los términos previstos en su normativa.

Se establece el régimen jurídico de las fundaciones del sector público estatal, manteniendo las líneas fundamentales de la Ley 50/2002, de 26 de diciembre, de Fundaciones. La creación de las fundaciones, o la adquisición de forma sobrevenida de esta forma jurídica, se efectuará por ley. Se deberá prever la posibilidad de que en el patrimonio de las fundaciones del sector público estatal pueda existir aportación del sector privado de forma no mayoritaria. Como novedad, se establece con carácter básico el régimen de adscripción pública de las fundaciones y del protectorado.

Se regulan por último en este Título los fondos carentes de personalidad jurídica del sector público estatal, figura cuya frecuente utilización demandaba el establecimiento de un régimen jurídico, y que deberán crearse por ley.

VI

El Título III establece un régimen completo de las relaciones entre las distintas Administraciones Públicas, que deberán sujetarse a nuevos principios rectores cuya última ratio se halla en los artículos 2, 14 y 138 de la Constitución, como la adecuación al sistema de distribución de competencias, la solidaridad interterritorial, la programación y evaluación de resultados y el respeto a la igualdad de derechos de todos los ciudadanos.

Siguiendo la jurisprudencia constitucional, se definen y diferencian dos principios clave de las relaciones entre Administraciones: la cooperación, que es voluntaria y la coordinación, que es obligatoria. Sobre esta base se regulan los diferentes órganos y formas de cooperar y coordinar.

Se desarrollan ampliamente las técnicas de cooperación y en especial, las de naturaleza orgánica, entre las que destaca la Conferencia de Presidentes, que se regula por primera vez, las Conferencias Sectoriales y las Comisiones Bilaterales de Cooperación. Dentro de las funciones de las Conferencias Sectoriales destaca como novedad la de ser informadas sobre anteproyectos de leyes y los proyectos de reglamentos del Gobierno de la Nación o de los Consejos de Gobierno de las Comunidades Autónomas, cuando afecten de manera directa al ámbito competencial de las otras Administraciones Públicas o cuando así esté previsto en la normativa sectorial aplicable. Con ello se pretende potenciar la planificación conjunta y evitar la aparición de duplicidades.

Se aclara que las Conferencias Sectoriales podrán adoptar recomendaciones, que implican el compromiso de quienes hayan votado a favor a orientar sus actuaciones en esa materia en el sentido acordado, con la obligación de motivar su no seguimiento; y acuerdos, que podrán adoptar la forma de planes conjuntos, que serán de obligado cumplimiento para todos los miembros no discrepantes, y que serán exigibles ante el orden jurisdiccional contencioso-administrativo. Cuando la Administración General del Estado ejerza funciones de coordinación, de acuerdo con la jurisprudencia constitucional, el acuerdo será obligatorio para todas las Administraciones de la conferencia sectorial.

Se prevé el posible funcionamiento electrónico de estos órganos, lo que favorecerá las convocatorias de las Conferencias Sectoriales, que podrán ser más frecuentes, ahorrando costes de desplazamiento.

Dentro del deber de colaboración se acotan los supuestos en los que la asistencia y cooperación puede negarse por parte de la Administración requerida, y se concretan las técnicas de colaboración: la creación y mantenimiento de sistemas integrados de información; el deber de asistencia y auxilio para atender las solicitudes formuladas por otras Administraciones para el mejor ejercicio de sus competencias y cualquier otra prevista en la Ley. No obstante, el deber de colaboración al que están sometidas las Administraciones Públicas se ejercerá con sometimiento a lo establecido en la normativa específica aplicable.

Se crea un Registro Electrónico estatal de Órganos e Instrumentos de Cooperación, con efecto constitutivo, de forma que pueda ser de general conocimiento, de forma fiable, la información relativa a los órganos de cooperación y coordinación en los que participa la Administración General del Estado y sus organismos públicos y entidades vinculados o dependientes, y qué convenios hay en vigor en cada momento.

Se da también respuesta legal a las interrelaciones competenciales que se han venido desarrollando durante los últimos años, propiciando la creación voluntaria de servicios integrados o complementarios, en los que cada Administración tenga en cuenta las competencias de otras Administraciones Públicas y conozca sus proyectos de actuación para mejorar la eficacia de todo el sistema administrativo.

También se potencia la disponibilidad de sistemas electrónicos de información mutua, cada vez más integrados, tal como se ha puesto de relieve con la Ley 20/2013, de 9 de diciembre, de garantía de la unidad de mercado.

En las disposiciones adicionales de la Ley se recogen, entre otras materias, la mención a la Administración de los Territorios Históricos del País Vasco, los Delegados del Gobierno en las Ciudades de Ceuta y Melilla, la estructura administrativa en las islas menores, las relaciones con las ciudades de Ceuta y Melilla, la adaptación de organismos públicos y entidades existentes, la gestión compartida de servicios comunes de los organismos públicos existentes, la transformación de los medios propios existentes, el Registro estatal de órganos e instrumentos de cooperación, la adaptación de los convenios vigentes, la Comisión sectorial de administración electrónica, la adaptación a los consorcios en los que participa el Estado, los conflictos de atribuciones intraministeriales, así como el régimen jurídico del Banco de España, las Autoridades Portuarias y Puertos del Estado, las entidades gestoras y servicios comunes de la Seguridad Social, la Agencia Estatal de Administración Tributaria y la organización militar, únicos cuyas peculiaridades justifican un tratamiento separado.

En las disposiciones transitorias se establece el régimen aplicable al sector público institucional existente en la entrada en vigor de la Ley, así como las reglas aplicables a los procedimientos de elaboración de normas en curso.

En la disposición derogatoria única se recoge la normativa y las disposiciones de igual o inferior rango que quedan derogadas.

Entre las disposiciones finales se incluye la modificación de la regulación del Gobierno contenida en la Ley 50/1997, de 27 de noviembre; también se modifica la Ley 33/2003, de 3 de noviembre; se establecen los títulos competenciales en base a los cuales se dicta la Ley, la habilitación para su desarrollo normativo; y la entrada en vigor, prevista para un año después de la publicación de la Ley en el «Boletín Oficial del Estado».

Las modificaciones introducidas en la actual Ley del Gobierno suponen una serie de trascendentes novedades. Así, se adecúa el régimen de los miembros del Gobierno a las previsiones de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado. En cuanto al Presidente del Gobierno, a los Vicepresidentes y a los Ministros, se introducen mejoras técnicas sobre el procedimiento y formalidades del cese. En el caso de que existan Ministros sin cartera, por Real Decreto se determinará el ámbito de sus competencias, la estructura administrativa, así como los medios materiales y personales que queden adscritos a dichos órganos.

Además de ello, se prevé excepcionalmente la asistencia de otros altos cargos al Consejo de Ministros, cuando sean convocados, posibilidad que hasta ahora solo se contemplaba respecto de los Secretarios de Estado.

Se flexibiliza el régimen de la suplencia de los miembros del Consejo de Ministros, ya que no se considerará ausencia la interrupción transitoria de la asistencia de los Ministros a las reuniones de un órgano colegiado. En tales casos, las funciones que pudieran

corresponder al miembro del Gobierno durante esa situación serán ejercidas por la siguiente autoridad en rango presente.

El Real Decreto de creación de cada una de las Comisiones Delegadas del Gobierno deberá regular, además de otras cuestiones, el régimen interno de funcionamiento y, en particular, el de convocatorias y suplencias. De esta manera, se completa el régimen de tales órganos.

Se contempla asimismo una habilitación al Gobierno para que defina determinadas cuestiones, como son la regulación de las precedencias en los actos oficiales de los titulares de los poderes constitucionales y de las instituciones nacionales, autonómicas, los Departamentos ministeriales y los órganos internos de estos, así como el régimen de los expresidentes del Gobierno.

De acuerdo con el propósito de que la tramitación telemática alcance todos los niveles del Gobierno, se prevé que el Ministro de la Presidencia pueda dictar instrucciones para la tramitación de asuntos ante los órganos colegiados del Gobierno que regulen la posible documentación de propuestas y acuerdos por medios electrónicos.

Los órganos de colaboración y apoyo al Gobierno siguen siendo los mismos que en la normativa actual: Comisión General de Secretarios de Estado y Subsecretarios, Secretariado del Gobierno y Gabinetes del Presidente del Gobierno, de los Vicepresidentes, de los Ministros y de los Secretarios de Estado. La Ley introduce mejoras en el funcionamiento de estos órganos, en particular, atribuyendo a la Comisión General de Secretarios de Estado y Subsecretarios el análisis o discusión de aquellos asuntos que, sin ser competencia del Consejo de Ministros o sus Comisiones Delegadas, afecten a varios Ministerios y sean sometidos a la Comisión por su Presidente.

Se recogen también a nivel legal las funciones del Secretariado del Gobierno como órgano de apoyo del Ministro de la Presidencia, del Consejo de Ministros, de las Comisiones Delegadas del Gobierno y de la Comisión General de Secretarios de Estado y Subsecretarios, y se le encomiendan otras que están relacionadas con la tramitación administrativa de la sanción y promulgación real de las Leyes, la expedición de los Reales Decretos, la tramitación de los actos y disposiciones del Rey cuyo refrendo corresponde al Presidente del Gobierno o al Presidente del Congreso de los Diputados y la tramitación de los actos y disposiciones que el ordenamiento jurídico atribuye a la competencia del Presidente del Gobierno, entre otras.

En cuanto al régimen de funcionamiento del Consejo de Ministros, destaca como novedad la regulación de la posibilidad de avocar, a propuesta del Presidente del Gobierno, las competencias cuya decisión corresponda a las Comisiones Delegadas del Gobierno.

Por último, se modifica el Título V de la Ley del Gobierno, con dos finalidades.

En primer lugar, se reforma el procedimiento a través del cual se ejerce la iniciativa legislativa y la potestad reglamentaria, en línea con los principios establecidos con carácter general para todas las Administraciones en la Ley de Procedimiento Administrativo y que entrañan la elaboración de un Plan Anual Normativo; la realización de una consulta pública con anterioridad a la redacción de las propuestas; el reforzamiento del contenido de la Memoria del Análisis de Impacto Normativo; la atribución de funciones al Ministerio de la Presidencia para asegurar la calidad normativa; y la evaluación ex post de las normas aprobadas.

Estas importantes novedades, tributarias de las iniciativas llevadas a cabo sobre Better Regulation en la Unión Europea, siguen asimismo las recomendaciones que en esta materia ha formulado la Organización para la Cooperación y el Desarrollo Económicos (OCDE) en su informe emitido en 2014 «Spain: From Administrative Reform to Continous Improvement». Es la Comunicación de la Comisión Europea al Consejo de 25 de junio de 2008 (A «Small Bussiness Act» for Europe) la que entre sus recomendaciones incluye la de fijar fechas concretas de entrada en vigor de cualquier norma que afecte a las pequeñas y medianas empresas, propuesta que se incorpora a la normativa estatal y que contribuirá a incrementar la seguridad jurídica en nuestra actividad económica.

En segundo lugar, se extrae el artículo dedicado al control del Gobierno del Título V, en el que impropiamente se encontraba, de modo que pasa a constituir uno específico con este exclusivo contenido, con una redacción mas acorde con la normativa reguladora de la jurisdicción contencioso-administrativa.

TÍTULO PRELIMINAR

Disposiciones generales, principios de actuación y funcionamiento del sector público

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley establece y regula las bases del régimen jurídico de las Administraciones Públicas, los principios del sistema de responsabilidad de las Administraciones Públicas y de la potestad sancionadora, así como la organización y funcionamiento de la Administración General del Estado y de su sector público institucional para el desarrollo de sus actividades.

Artículo 2. *Ámbito Subjetivo.*

1. La presente Ley se aplica al sector público que comprende:

a) La Administración General del Estado.
b) Las Administraciones de las Comunidades Autónomas.
c) Las Entidades que integran la Administración Local.
d) El sector público institucional.

2. El sector público institucional se integra por:

a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.
b) Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas que quedarán sujetas a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, en particular a los principios previstos en el artículo 3, y en todo caso, cuando ejerzan potestades administrativas.
c) Las Universidades públicas que se regirán por su normativa específica y supletoriamente por las previsiones de la presente Ley.

3. Tienen la consideración de Administraciones Públicas la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2.

Artículo 3. *Principios generales.*

1. Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho.
Deberán respetar en su actuación y relaciones los siguientes principios:

a) Servicio efectivo a los ciudadanos.
b) Simplicidad, claridad y proximidad a los ciudadanos.
c) Participación, objetividad y transparencia de la actuación administrativa.
d) Racionalización y agilidad de los procedimientos administrativos y de las actividades materiales de gestión.
e) Buena fe, confianza legítima y lealtad institucional.
f) Responsabilidad por la gestión pública.
g) Planificación y dirección por objetivos y control de la gestión y evaluación de los resultados de las políticas públicas.
h) Eficacia en el cumplimiento de los objetivos fijados.
i) Economía, suficiencia y adecuación estricta de los medios a los fines institucionales.
j) Eficiencia en la asignación y utilización de los recursos públicos.
k) Cooperación, colaboración y coordinación entre las Administraciones Públicas.

2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

3. Bajo la dirección del Gobierno de la Nación, de los órganos de gobierno de las Comunidades Autónomas y de los correspondientes de las Entidades Locales, la actuación de la Administración Pública respectiva se desarrolla para alcanzar los objetivos que establecen las leyes y el resto del ordenamiento jurídico.

4. Cada una de las Administraciones Públicas del artículo 2 actúa para el cumplimiento de sus fines con personalidad jurídica única.

Artículo 4. *Principios de intervención de las Administraciones Públicas para el desarrollo de una actividad.*

1. Las Administraciones Públicas que, en el ejercicio de sus respectivas competencias, establezcan medidas que limiten el ejercicio de derechos individuales o colectivos o exijan el cumplimiento de requisitos para el desarrollo de una actividad, deberán aplicar el principio de proporcionalidad y elegir la medida menos restrictiva, motivar su necesidad para la protección del interés público así como justificar su adecuación para lograr los fines que se persiguen, sin que en ningún caso se produzcan diferencias de trato discriminatorias. Asimismo deberán evaluar periódicamente los efectos y resultados obtenidos.

2. Las Administraciones Públicas velarán por el cumplimiento de los requisitos previstos en la legislación que resulte aplicable, para lo cual podrán, en el ámbito de sus respectivas competencias y con los límites establecidos en la legislación de protección de datos de carácter personal, comprobar, verificar, investigar e inspeccionar los hechos, actos, elementos, actividades, estimaciones y demás circunstancias que fueran necesarias.

CAPÍTULO II

De los órganos de las Administraciones Públicas

Sección 1.ª De los órganos administrativos

Artículo 5. *Órganos administrativos.*

1. Tendrán la consideración de órganos administrativos las unidades administrativas a las que se les atribuyan funciones que tengan efectos jurídicos frente a terceros, o cuya actuación tenga carácter preceptivo.

2. Corresponde a cada Administración Pública delimitar, en su respectivo ámbito competencial, las unidades administrativas que configuran los órganos administrativos propios de las especialidades derivadas de su organización.

3. La creación de cualquier órgano administrativo exigirá, al menos, el cumplimiento de los siguientes requisitos:

a) Determinación de su forma de integración en la Administración Pública de que se trate y su dependencia jerárquica.

b) Delimitación de sus funciones y competencias.

c) Dotación de los créditos necesarios para su puesta en marcha y funcionamiento.

4. No podrán crearse nuevos órganos que supongan duplicación de otros ya existentes si al mismo tiempo no se suprime o restringe debidamente la competencia de estos. A este objeto, la creación de un nuevo órgano sólo tendrá lugar previa comprobación de que no existe otro en la misma Administración Pública que desarrolle igual función sobre el mismo territorio y población.

Artículo 6. *Instrucciones y órdenes de servicio.*

1. Los órganos administrativos podrán dirigir las actividades de sus órganos jerárquicamente dependientes mediante instrucciones y órdenes de servicio.

Cuando una disposición específica así lo establezca, o se estime conveniente por razón de los destinatarios o de los efectos que puedan producirse, las instrucciones y órdenes de servicio se publicarán en el boletín oficial que corresponda, sin perjuicio de su difusión de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

2. El incumplimiento de las instrucciones u órdenes de servicio no afecta por sí solo a la validez de los actos dictados por los órganos administrativos, sin perjuicio de la responsabilidad disciplinaria en que se pueda incurrir.

Artículo 7. *Órganos consultivos.*

La Administración consultiva podrá articularse mediante órganos específicos dotados de autonomía orgánica y funcional con respecto a la Administración activa, o a través de los servicios de esta última que prestan asistencia jurídica.

En tal caso, dichos servicios no podrán estar sujetos a dependencia jerárquica, ya sea orgánica o funcional, ni recibir instrucciones, directrices o cualquier clase de indicación de los órganos que hayan elaborado las disposiciones o producido los actos objeto de consulta, actuando para cumplir con tales garantías de forma colegiada.

Sección 2.ª Competencia

Artículo 8. *Competencia.*

1. La competencia es irrenunciable y se ejercerá por los órganos administrativos que la tengan atribuida como propia, salvo los casos de delegación o avocación, cuando se efectúen en los términos previstos en ésta u otras leyes.

La delegación de competencias, las encomiendas de gestión, la delegación de firma y la suplencia no suponen alteración de la titularidad de la competencia, aunque sí de los elementos determinantes de su ejercicio que en cada caso se prevén.

2. La titularidad y el ejercicio de las competencias atribuidas a los órganos administrativos podrán ser desconcentradas en otros jerárquicamente dependientes de aquéllos en los términos y con los requisitos que prevean las propias normas de atribución de competencias.

3. Si alguna disposición atribuye la competencia a una Administración, sin especificar el órgano que debe ejercerla, se entenderá que la facultad de instruir y resolver los expedientes corresponde a los órganos inferiores competentes por razón de la materia y del territorio. Si existiera más de un órgano inferior competente por razón de materia y territorio, la facultad para instruir y resolver los expedientes corresponderá al superior jerárquico común de estos.

Artículo 9. *Delegación de competencias.*

1. Los órganos de las diferentes Administraciones Públicas podrán delegar el ejercicio de las competencias que tengan atribuidas en otros órganos de la misma Administración, aun cuando no sean jerárquicamente dependientes, o en los Organismos públicos o Entidades de Derecho Público vinculados o dependientes de aquéllas.

En el ámbito de la Administración General del Estado, la delegación de competencias deberá ser aprobada previamente por el órgano ministerial de quien dependa el órgano delegante y en el caso de los Organismos públicos o Entidades vinculados o dependientes, por el órgano máximo de dirección, de acuerdo con sus normas de creación. Cuando se trate de órganos no relacionados jerárquicamente será necesaria la aprobación previa del superior común si ambos pertenecen al mismo Ministerio, o del órgano superior de quien dependa el órgano delegado, si el delegante y el delegado pertenecen a diferentes Ministerios.

Asimismo, los órganos de la Administración General del Estado podrán delegar el ejercicio de sus competencias propias en sus Organismos públicos y Entidades vinculados o dependientes, cuando resulte conveniente para alcanzar los fines que tengan asignados y mejorar la eficacia de su gestión. La delegación deberá ser previamente aprobada por los órganos de los que dependan el órgano delegante y el órgano delegado, o aceptada por este

último cuando sea el órgano máximo de dirección del Organismo público o Entidad vinculado o dependiente.

2. En ningún caso podrán ser objeto de delegación las competencias relativas a:

a) Los asuntos que se refieran a relaciones con la Jefatura del Estado, la Presidencia del Gobierno de la Nación, las Cortes Generales, las Presidencias de los Consejos de Gobierno de las Comunidades Autónomas y las Asambleas Legislativas de las Comunidades Autónomas.

b) La adopción de disposiciones de carácter general.

c) La resolución de recursos en los órganos administrativos que hayan dictado los actos objeto de recurso.

d) Las materias en que así se determine por norma con rango de Ley.

3. Las delegaciones de competencias y su revocación deberán publicarse en el «Boletín Oficial del Estado», en el de la Comunidad Autónoma o en el de la Provincia, según la Administración a que pertenezca el órgano delegante, y el ámbito territorial de competencia de éste.

4. Las resoluciones administrativas que se adopten por delegación indicarán expresamente esta circunstancia y se considerarán dictadas por el órgano delegante.

5. Salvo autorización expresa de una Ley, no podrán delegarse las competencias que se ejerzan por delegación.

No constituye impedimento para que pueda delegarse la competencia para resolver un procedimiento la circunstancia de que la norma reguladora del mismo prevea, como trámite preceptivo, la emisión de un dictamen o informe; no obstante, no podrá delegarse la competencia para resolver un procedimiento una vez que en el correspondiente procedimiento se haya emitido un dictamen o informe preceptivo acerca del mismo.

6. La delegación será revocable en cualquier momento por el órgano que la haya conferido.

7. El acuerdo de delegación de aquellas competencias atribuidas a órganos colegiados, para cuyo ejercicio se requiera un quórum o mayoría especial, deberá adoptarse observando, en todo caso, dicho quórum o mayoría.

Artículo 10. *Avocación.*

1. Los órganos superiores podrán avocar para sí el conocimiento de uno o varios asuntos cuya resolución corresponda ordinariamente o por delegación a sus órganos administrativos dependientes, cuando circunstancias de índole técnica, económica, social, jurídica o territorial lo hagan conveniente.

En los supuestos de delegación de competencias en órganos no dependientes jerárquicamente, el conocimiento de un asunto podrá ser avocado únicamente por el órgano delegante.

2. En todo caso, la avocación se realizará mediante acuerdo motivado que deberá ser notificado a los interesados en el procedimiento, si los hubiere, con anterioridad o simultáneamente a la resolución final que se dicte.

Contra el acuerdo de avocación no cabrá recurso, aunque podrá impugnarse en el que, en su caso, se interponga contra la resolución del procedimiento.

Artículo 11. *Encomiendas de gestión.*

1. La realización de actividades de carácter material o técnico de la competencia de los órganos administrativos o de las Entidades de Derecho Público podrá ser encomendada a otros órganos o Entidades de Derecho Público de la misma o de distinta Administración, siempre que entre sus competencias estén esas actividades, por razones de eficacia o cuando no se posean los medios técnicos idóneos para su desempeño.

Las encomiendas de gestión no podrán tener por objeto prestaciones propias de los contratos regulados en la legislación de contratos del sector público. En tal caso, su naturaleza y régimen jurídico se ajustará a lo previsto en ésta.

2. La encomienda de gestión no supone cesión de la titularidad de la competencia ni de los elementos sustantivos de su ejercicio, siendo responsabilidad del órgano o Entidad

encomendante dictar cuantos actos o resoluciones de carácter jurídico den soporte o en los que se integre la concreta actividad material objeto de encomienda.

En todo caso, la Entidad u órgano encomendado tendrá la condición de encargado del tratamiento de los datos de carácter personal a los que pudiera tener acceso en ejecución de la encomienda de gestión, siéndole de aplicación lo dispuesto en la normativa de protección de datos de carácter personal.

3. La formalización de las encomiendas de gestión se ajustará a las siguientes reglas:

a) Cuando la encomienda de gestión se realice entre órganos administrativos o Entidades de Derecho Público pertenecientes a la misma Administración deberá formalizarse en los términos que establezca su normativa propia y, en su defecto, por acuerdo expreso de los órganos o Entidades de Derecho Público intervinientes. En todo caso, el instrumento de formalización de la encomienda de gestión y su resolución deberá ser publicada, para su eficacia, en el Boletín Oficial del Estado, en el Boletín oficial de la Comunidad Autónoma o en el de la Provincia, según la Administración a que pertenezca el órgano encomendante.

Cada Administración podrá regular los requisitos necesarios para la validez de tales acuerdos que incluirán, al menos, expresa mención de la actividad o actividades a las que afecten, el plazo de vigencia y la naturaleza y alcance de la gestión encomendada.

b) Cuando la encomienda de gestión se realice entre órganos y Entidades de Derecho Público de distintas Administraciones se formalizará mediante firma del correspondiente convenio entre ellas, que deberá ser publicado en el «Boletín Oficial del Estado», en el Boletín oficial de la Comunidad Autónoma o en el de la Provincia, según la Administración a que pertenezca el órgano encomendante, salvo en el supuesto de la gestión ordinaria de los servicios de las Comunidades Autónomas por las Diputaciones Provinciales o en su caso Cabildos o Consejos insulares, que se regirá por la legislación de Régimen Local.

Artículo 12. *Delegación de firma.*

1. Los titulares de los órganos administrativos podrán, en materias de su competencia, que ostenten, bien por atribución, bien por delegación de competencias, delegar la firma de sus resoluciones y actos administrativos en los titulares de los órganos o unidades administrativas que de ellos dependan, dentro de los límites señalados en el artículo 9.

2. La delegación de firma no alterará la competencia del órgano delegante y para su validez no será necesaria su publicación.

3. En las resoluciones y actos que se firmen por delegación se hará constar esta circunstancia y la autoridad de procedencia.

Artículo 13. *Suplencia.*

1. En la forma que disponga cada Administración Pública, los titulares de los órganos administrativos podrán ser suplidos temporalmente en los supuestos de vacante, ausencia o enfermedad, así como en los casos en que haya sido declarada su abstención o recusación.

Si no se designa suplente, la competencia del órgano administrativo se ejercerá por quien designe el órgano administrativo inmediato superior de quien dependa.

2. La suplencia no implicará alteración de la competencia y para su validez no será necesaria su publicación.

3. En el ámbito de la Administración General del Estado, la designación de suplente podrá efectuarse:

a) En los reales decretos de estructura orgánica básica de los Departamentos Ministeriales o en los estatutos de sus Organismos públicos y Entidades vinculados o dependientes según corresponda.

b) Por el órgano competente para el nombramiento del titular, bien en el propio acto de nombramiento bien en otro posterior cuando se produzca el supuesto que dé lugar a la suplencia.

4. En las resoluciones y actos que se dicten mediante suplencia, se hará constar esta circunstancia y se especificará el titular del órgano en cuya suplencia se adoptan y quien efectivamente está ejerciendo esta suplencia.

Artículo 14. *Decisiones sobre competencia.*

1. El órgano administrativo que se estime incompetente para la resolución de un asunto remitirá directamente las actuaciones al órgano que considere competente, debiendo notificar esta circunstancia a los interesados.

2. Los interesados que sean parte en el procedimiento podrán dirigirse al órgano que se encuentre conociendo de un asunto para que decline su competencia y remita las actuaciones al órgano competente.

Asimismo, podrán dirigirse al órgano que estimen competente para que requiera de inhibición al que esté conociendo del asunto.

3. Los conflictos de atribuciones sólo podrán suscitarse entre órganos de una misma Administración no relacionados jerárquicamente, y respecto a asuntos sobre los que no haya finalizado el procedimiento administrativo.

Sección 3.ª Órganos colegiados de las distintas administraciones públicas

Subsección 1.ª Funcionamiento

Artículo 15. *Régimen.*

1. El régimen jurídico de los órganos colegiados se ajustará a las normas contenidas en la presente sección, sin perjuicio de las peculiaridades organizativas de las Administraciones Públicas en que se integran.

2. Los órganos colegiados de las distintas Administraciones Públicas en que participen organizaciones representativas de intereses sociales, así como aquellos compuestos por representaciones de distintas Administraciones Públicas, cuenten o no con participación de organizaciones representativas de intereses sociales, podrán establecer o completar sus propias normas de funcionamiento.

Los órganos colegiados a que se refiere este apartado quedarán integrados en la Administración Pública que corresponda, aunque sin participar en la estructura jerárquica de ésta, salvo que así lo establezcan sus normas de creación, se desprenda de sus funciones o de la propia naturaleza del órgano colegiado.

3. El acuerdo de creación y las normas de funcionamiento de los órganos colegiados que dicten resoluciones que tengan efectos jurídicos frente a terceros deberán ser publicados en el Boletín o Diario Oficial de la Administración Pública en que se integran. Adicionalmente, las Administraciones podrán publicarlos en otros medios de difusión que garanticen su conocimiento.

Cuando se trate de un órgano colegiado a los que se refiere el apartado 2 de este artículo la citada publicidad se realizará por la Administración a quien corresponda la Presidencia.

Artículo 16. *Secretario.*

1. Los órganos colegiados tendrán un Secretario que podrá ser un miembro del propio órgano o una persona al servicio de la Administración Pública correspondiente.

2. Corresponderá al Secretario velar por la legalidad formal y material de las actuaciones del órgano colegiado, certificar las actuaciones del mismo y garantizar que los procedimientos y reglas de constitución y adopción de acuerdos son respetadas.

3. En caso de que el Secretario no miembro sea suplido por un miembro del órgano colegiado, éste conservará todos sus derechos como tal.

Artículo 17. *Convocatorias y sesiones.*

1. Todos los órganos colegiados se podrán constituir, convocar, celebrar sus sesiones, adoptar acuerdos y remitir actas tanto de forma presencial como a distancia, salvo que su reglamento interno recoja expresa y excepcionalmente lo contrario.

En las sesiones que celebren los órganos colegiados a distancia, sus miembros podrán encontrarse en distintos lugares siempre y cuando se asegure por medios electrónicos, considerándose también tales los telefónicos, y audiovisuales, la identidad de los miembros o personas que los suplan, el contenido de sus manifestaciones, el momento en que éstas

se producen, así como la interactividad e intercomunicación entre ellos en tiempo real y la disponibilidad de los medios durante la sesión. Entre otros, se considerarán incluidos entre los medios electrónicos válidos, el correo electrónico, las audioconferencias y las videoconferencias.

2. Para la válida constitución del órgano, a efectos de la celebración de sesiones, deliberaciones y toma de acuerdos, se requerirá la asistencia, presencial o a distancia, del Presidente y Secretario o en su caso, de quienes les suplan, y la de la mitad, al menos, de sus miembros.

Cuando se trate de los órganos colegiados a que se refiere el artículo 15.2, el Presidente podrá considerar válidamente constituido el órgano, a efectos de celebración de sesión, si asisten los representantes de las Administraciones Públicas y de las organizaciones representativas de intereses sociales miembros del órgano a los que se haya atribuido la condición de portavoces.

Cuando estuvieran reunidos, de manera presencial o a distancia, el Secretario y todos los miembros del órgano colegiado, o en su caso las personas que les suplan, éstos podrán constituirse válidamente como órgano colegiado para la celebración de sesiones, deliberaciones y adopción de acuerdos sin necesidad de convocatoria previa cuando así lo decidan todos sus miembros.

3. Los órganos colegiados podrán establecer el régimen propio de convocatorias, si éste no está previsto por sus normas de funcionamiento. Tal régimen podrá prever una segunda convocatoria y especificar para ésta el número de miembros necesarios para constituir válidamente el órgano.

Salvo que no resulte posible, las convocatorias serán remitidas a los miembros del órgano colegiado a través de medios electrónicos, haciendo constar en la misma el orden del día junto con la documentación necesaria para su deliberación cuando sea posible, las condiciones en las que se va a celebrar la sesión, el sistema de conexión y, en su caso, los lugares en que estén disponibles los medios técnicos necesarios para asistir y participar en la reunión.

4. No podrá ser objeto de deliberación o acuerdo ningún asunto que no figure incluido en el orden del día, salvo que asistan todos los miembros del órgano colegiado y sea declarada la urgencia del asunto por el voto favorable de la mayoría.

5. Los acuerdos serán adoptados por mayoría de votos. Cuando se asista a distancia, los acuerdos se entenderán adoptados en el lugar donde tenga la sede el órgano colegiado y, en su defecto, donde esté ubicada la presidencia.

6. Cuando los miembros del órgano voten en contra o se abstengan, quedarán exentos de la responsabilidad que, en su caso, pueda derivarse de los acuerdos.

7. Quienes acrediten la titularidad de un interés legítimo podrán dirigirse al Secretario de un órgano colegiado para que les sea expedida certificación de sus acuerdos. La certificación será expedida por medios electrónicos, salvo que el interesado manifieste expresamente lo contrario y no tenga obligación de relacionarse con las Administraciones por esta vía.

Artículo 18. *Actas.*

1. De cada sesión que celebre el órgano colegiado se levantará acta por el Secretario, que especificará necesariamente los asistentes, el orden del día de la reunión, las circunstancias del lugar y tiempo en que se ha celebrado, los puntos principales de las deliberaciones, así como el contenido de los acuerdos adoptados.

Podrán grabarse las sesiones que celebre el órgano colegiado. El fichero resultante de la grabación, junto con la certificación expedida por el Secretario de la autenticidad e integridad del mismo, y cuantos documentos en soporte electrónico se utilizasen como documentos de la sesión, podrán acompañar al acta de las sesiones, sin necesidad de hacer constar en ella los puntos principales de las deliberaciones.

2. El acta de cada sesión podrá aprobarse en la misma reunión o en la inmediata siguiente. El Secretario elaborará el acta con el visto bueno del Presidente y lo remitirá a través de medios electrónicos, a los miembros del órgano colegiado, quienes podrán manifestar por los mismos medios su conformidad o reparos al texto, a efectos de su aprobación, considerándose, en caso afirmativo, aprobada en la misma reunión.

Cuando se hubiese optado por la grabación de las sesiones celebradas o por la utilización de documentos en soporte electrónico, deberán conservarse de forma que se garantice la integridad y autenticidad de los ficheros electrónicos correspondientes y el acceso a los mismos por parte de los miembros del órgano colegiado.

Subsección 2.ª De los órganos colegiados en la Administración General del Estado

Artículo 19. *Régimen de los órganos colegiados de la Administración General del Estado y de las Entidades de Derecho Público vinculadas o dependientes de ella.*

1. Los órganos colegiados de la Administración General del Estado y de las Entidades de Derecho Público vinculadas o dependientes de ella, se regirán por las normas establecidas en este artículo, y por las previsiones que sobre ellos se establecen en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas.

2. Corresponderá a su Presidente:

a) Ostentar la representación del órgano.

b) Acordar la convocatoria de las sesiones ordinarias y extraordinarias y la fijación del orden del día, teniendo en cuenta, en su caso, las peticiones de los demás miembros, siempre que hayan sido formuladas con la suficiente antelación.

c) Presidir las sesiones, moderar el desarrollo de los debates y suspenderlos por causas justificadas.

d) Dirimir con su voto los empates, a efectos de adoptar acuerdos, excepto si se trata de los órganos colegiados a que se refiere el artículo 15.2, en los que el voto será dirimente si así lo establecen sus propias normas.

e) Asegurar el cumplimiento de las leyes.

f) Visar las actas y certificaciones de los acuerdos del órgano.

g) Ejercer cuantas otras funciones sean inherentes a su condición de Presidente del órgano.

En casos de vacante, ausencia, enfermedad, u otra causa legal, el Presidente será sustituido por el Vicepresidente que corresponda, y en su defecto, por el miembro del órgano colegiado de mayor jerarquía, antigüedad y edad, por este orden.

Esta norma no será de aplicación a los órganos colegiados previstos en el artículo 15.2 en los que el régimen de sustitución del Presidente debe estar específicamente regulado en cada caso, o establecido expresamente por acuerdo del Pleno del órgano colegiado.

3. Los miembros del órgano colegiado deberán:

a) Recibir, con una antelación mínima de dos días, la convocatoria conteniendo el orden del día de las reuniones. La información sobre los temas que figuren en el orden del día estará a disposición de los miembros en igual plazo.

b) Participar en los debates de las sesiones.

c) Ejercer su derecho al voto y formular su voto particular, así como expresar el sentido de su voto y los motivos que lo justifican. No podrán abstenerse en las votaciones quienes por su cualidad de autoridades o personal al servicio de las Administraciones Públicas, tengan la condición de miembros natos de órganos colegiados, en virtud del cargo que desempeñan.

d) Formular ruegos y preguntas.

e) Obtener la información precisa para cumplir las funciones asignadas.

f) Cuantas otras funciones sean inherentes a su condición.

Los miembros de un órgano colegiado no podrán atribuirse las funciones de representación reconocidas a éste, salvo que expresamente se les hayan otorgado por una norma o por acuerdo válidamente adoptado, para cada caso concreto, por el propio órgano.

En casos de ausencia o de enfermedad y, en general, cuando concurra alguna causa justificada, los miembros titulares del órgano colegiado serán sustituidos por sus suplentes, si los hubiera.

Cuando se trate de órganos colegiados a los que se refiere el artículo 15 las organizaciones representativas de intereses sociales podrán sustituir a sus miembros

titulares por otros, acreditándolo ante la Secretaría del órgano colegiado, con respeto a las reservas y limitaciones que establezcan sus normas de organización.

Los miembros del órgano colegiado no podrán ejercer estas funciones cuando concurra conflicto de interés.

4. La designación y el cese, así como la sustitución temporal del Secretario en supuestos de vacante, ausencia o enfermedad se realizarán según lo dispuesto en las normas específicas de cada órgano y, en su defecto, por acuerdo del mismo.

Corresponde al Secretario del órgano colegiado:

a) Asistir a las reuniones con voz pero sin voto, y con voz y voto si la Secretaría del órgano la ostenta un miembro del mismo.

b) Efectuar la convocatoria de las sesiones del órgano por orden del Presidente, así como las citaciones a los miembros del mismo.

c) Recibir los actos de comunicación de los miembros con el órgano, sean notificaciones, peticiones de datos, rectificaciones o cualquiera otra clase de escritos de los que deba tener conocimiento.

d) Preparar el despacho de los asuntos, redactar y autorizar las actas de las sesiones.

e) Expedir certificaciones de las consultas, dictámenes y acuerdos aprobados.

f) Cuantas otras funciones sean inherentes a su condición de Secretario.

5. En el acta figurará, a solicitud de los respectivos miembros del órgano, el voto contrario al acuerdo adoptado, su abstención y los motivos que la justifiquen o el sentido de su voto favorable.

Asimismo, cualquier miembro tiene derecho a solicitar la transcripción íntegra de su intervención o propuesta, siempre que, en ausencia de grabación de la reunión aneja al acta, aporte en el acto, o en el plazo que señale el Presidente, el texto que se corresponda fielmente con su intervención, haciéndose así constar en el acta o uniéndose copia a la misma.

Los miembros que discrepen del acuerdo mayoritario podrán formular voto particular por escrito en el plazo de dos días, que se incorporará al texto aprobado.

Las actas se aprobarán en la misma o en la siguiente sesión, pudiendo no obstante emitir el Secretario certificación sobre los acuerdos que se hayan adoptado, sin perjuicio de la ulterior aprobación del acta. Se considerará aprobada en la misma sesión el acta que, con posterioridad a la reunión, sea distribuida entre los miembros y reciba la conformidad de éstos por cualquier medio del que el Secretario deje expresión y constancia.

En las certificaciones de acuerdos adoptados emitidas con anterioridad a la aprobación del acta se hará constar expresamente tal circunstancia.

Artículo 20. *Requisitos para constituir órganos colegiados.*

1. Son órganos colegiados aquellos que se creen formalmente y estén integrados por tres o más personas, a los que se atribuyan funciones administrativas de decisión, propuesta, asesoramiento, seguimiento o control, y que actúen integrados en la Administración General del Estado o alguno de sus Organismos públicos.

2. La constitución de un órgano colegiado en la Administración General del Estado y en sus Organismos públicos tiene como presupuesto indispensable la determinación en su norma de creación o en el convenio con otras Administraciones Públicas por el que dicho órgano se cree, de los siguientes extremos:

a) Sus fines u objetivos.

b) Su integración administrativa o dependencia jerárquica.

c) La composición y los criterios para la designación de su Presidente y de los restantes miembros.

d) Las funciones de decisión, propuesta, informe, seguimiento o control, así como cualquier otra que se le atribuya.

e) La dotación de los créditos necesarios, en su caso, para su funcionamiento.

3. El régimen jurídico de los órganos colegiados a que se refiere el apartado 1 de este artículo se ajustará a las normas contenidas en el artículo 19, sin perjuicio de las

peculiaridades organizativas contenidas en la presente Ley o en su norma o convenio de creación.

Artículo 21. *Clasificación y composición de los órganos colegiados.*

1. Los órganos colegiados de la Administración General del Estado y de sus Organismos públicos, por su composición, se clasifican en:

a) Órganos colegiados interministeriales, si sus miembros proceden de diferentes Ministerios.
b) Órganos colegiados ministeriales, si sus componentes proceden de los órganos de un solo Ministerio.

2. En los órganos colegiados a los que se refiere el apartado anterior, podrá haber representantes de otras Administraciones Públicas, cuando éstas lo acepten voluntariamente, cuando un convenio así lo establezca o cuando una norma aplicable a las Administraciones afectadas lo determine.
3. En la composición de los órganos colegiados podrán participar, cuando así se determine, organizaciones representativas de intereses sociales, así como otros miembros que se designen por las especiales condiciones de experiencia o conocimientos que concurran en ellos, en atención a la naturaleza de las funciones asignadas a tales órganos.

Artículo 22. *Creación, modificación y supresión de órganos colegiados.*

1. La creación de órganos colegiados de la Administración General del Estado y de sus Organismos públicos sólo requerirá de norma específica, con publicación en el «Boletín Oficial del Estado», en los casos en que se les atribuyan cualquiera de las siguientes competencias:

a) Competencias decisorias.
b) Competencias de propuesta o emisión de informes preceptivos que deban servir de base a decisiones de otros órganos administrativos.
c) Competencias de seguimiento o control de las actuaciones de otros órganos de la Administración General del Estado.

2. En los supuestos enunciados en el apartado anterior, la norma de creación deberá revestir la forma de Real Decreto en el caso de los órganos colegiados interministeriales cuyo Presidente tenga rango superior al de Director general; Orden ministerial conjunta para los restantes órganos colegiados interministeriales, y Orden ministerial para los de este carácter.
3. En todos los supuestos no comprendidos en el apartado 1 de este artículo, los órganos colegiados tendrán el carácter de grupos o comisiones de trabajo y podrán ser creados por Acuerdo del Consejo de Ministros o por los Ministerios interesados. Sus acuerdos no podrán tener efectos directos frente a terceros.
4. La modificación y supresión de los órganos colegiados y de los grupos o comisiones de trabajo de la Administración General del Estado y de los Organismos públicos se llevará a cabo en la misma forma dispuesta para su creación, salvo que ésta hubiera fijado plazo previsto para su extinción, en cuyo caso ésta se producirá automáticamente en la fecha señalada al efecto.

Sección 4.ª Abstención y recusación

Artículo 23. *Abstención.*

1. Las autoridades y el personal al servicio de las Administraciones en quienes se den algunas de las circunstancias señaladas en el apartado siguiente se abstendrán de intervenir en el procedimiento y lo comunicarán a su superior inmediato, quien resolverá lo procedente.
2. Son motivos de abstención los siguientes:

a) Tener interés personal en el asunto de que se trate o en otro en cuya resolución pudiera influir la de aquél; ser administrador de sociedad o entidad interesada, o tener cuestión litigiosa pendiente con algún interesado.

b) Tener un vínculo matrimonial o situación de hecho asimilable y el parentesco de consanguinidad dentro del cuarto grado o de afinidad dentro del segundo, con cualquiera de los interesados, con los administradores de entidades o sociedades interesadas y también con los asesores, representantes legales o mandatarios que intervengan en el procedimiento, así como compartir despacho profesional o estar asociado con éstos para el asesoramiento, la representación o el mandato.

c) Tener amistad íntima o enemistad manifiesta con alguna de las personas mencionadas en el apartado anterior.

d) Haber intervenido como perito o como testigo en el procedimiento de que se trate.

e) Tener relación de servicio con persona natural o jurídica interesada directamente en el asunto, o haberle prestado en los dos últimos años servicios profesionales de cualquier tipo y en cualquier circunstancia o lugar.

3. Los órganos jerárquicamente superiores a quien se encuentre en alguna de las circunstancias señaladas en el punto anterior podrán ordenarle que se abstengan de toda intervención en el expediente.

4. La actuación de autoridades y personal al servicio de las Administraciones Públicas en los que concurran motivos de abstención no implicará, necesariamente, y en todo caso, la invalidez de los actos en que hayan intervenido.

5. La no abstención en los casos en que concurra alguna de esas circunstancias dará lugar a la responsabilidad que proceda.

Artículo 24. *Recusación.*

1. En los casos previstos en el artículo anterior, podrá promoverse recusación por los interesados en cualquier momento de la tramitación del procedimiento.

2. La recusación se planteará por escrito en el que se expresará la causa o causas en que se funda.

3. En el día siguiente el recusado manifestará a su inmediato superior si se da o no en él la causa alegada. En el primer caso, si el superior aprecia la concurrencia de la causa de recusación, acordará su sustitución acto seguido.

4. Si el recusado niega la causa de recusación, el superior resolverá en el plazo de tres días, previos los informes y comprobaciones que considere oportunos.

5. Contra las resoluciones adoptadas en esta materia no cabrá recurso, sin perjuicio de la posibilidad de alegar la recusación al interponer el recurso que proceda contra el acto que ponga fin al procedimiento.

CAPÍTULO III

Principios de la potestad sancionadora

Artículo 25. *Principio de legalidad.*

1. La potestad sancionadora de las Administraciones Públicas se ejercerá cuando haya sido expresamente reconocida por una norma con rango de Ley, con aplicación del procedimiento previsto para su ejercicio y de acuerdo con lo establecido en esta Ley y en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y, cuando se trate de Entidades Locales, de conformidad con lo dispuesto en el Título XI de la Ley 7/1985, de 2 de abril.

2. El ejercicio de la potestad sancionadora corresponde a los órganos administrativos que la tengan expresamente atribuida, por disposición de rango legal o reglamentario.

3. Las disposiciones de este Capítulo serán extensivas al ejercicio por las Administraciones Públicas de su potestad disciplinaria respecto del personal a su servicio, cualquiera que sea la naturaleza jurídica de la relación de empleo.

4. Las disposiciones de este capítulo no serán de aplicación al ejercicio por las Administraciones Públicas de la potestad sancionadora respecto de quienes estén vinculados a ellas por relaciones reguladas por la legislación de contratos del sector público o por la legislación patrimonial de las Administraciones Públicas.

Artículo 26. *Irretroactividad.*

1. Serán de aplicación las disposiciones sancionadoras vigentes en el momento de producirse los hechos que constituyan infracción administrativa.

2. Las disposiciones sancionadoras producirán efecto retroactivo en cuanto favorezcan al presunto infractor o al infractor, tanto en lo referido a la tipificación de la infracción como a la sanción y a sus plazos de prescripción, incluso respecto de las sanciones pendientes de cumplimiento al entrar en vigor la nueva disposición.

Artículo 27. *Principio de tipicidad.*

1. Sólo constituyen infracciones administrativas las vulneraciones del ordenamiento jurídico previstas como tales infracciones por una Ley, sin perjuicio de lo dispuesto para la Administración Local en el Título XI de la Ley 7/1985, de 2 de abril.

Las infracciones administrativas se clasificarán por la Ley en leves, graves y muy graves.

2. Únicamente por la comisión de infracciones administrativas podrán imponerse sanciones que, en todo caso, estarán delimitadas por la Ley.

3. Las disposiciones reglamentarias de desarrollo podrán introducir especificaciones o graduaciones al cuadro de las infracciones o sanciones establecidas legalmente que, sin constituir nuevas infracciones o sanciones, ni alterar la naturaleza o límites de las que la Ley contempla, contribuyan a la más correcta identificación de las conductas o a la más precisa determinación de las sanciones correspondientes.

4. Las normas definidoras de infracciones y sanciones no serán susceptibles de aplicación analógica.

Artículo 28. *Responsabilidad.*

1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa.

2. Las responsabilidades administrativas que se deriven de la comisión de una infracción serán compatibles con la exigencia al infractor de la reposición de la situación alterada por el mismo a su estado originario, así como con la indemnización por los daños y perjuicios causados, que será determinada y exigida por el órgano al que corresponda el ejercicio de la potestad sancionadora. De no satisfacerse la indemnización en el plazo que al efecto se determine en función de su cuantía, se procederá en la forma prevista en el artículo 101 de la Ley del Procedimiento Administrativo Común de las Administraciones Públicas.

3. Cuando el cumplimiento de una obligación establecida por una norma con rango de Ley corresponda a varias personas conjuntamente, responderán de forma solidaria de las infracciones que, en su caso, se cometan y de las sanciones que se impongan. No obstante, cuando la sanción sea pecuniaria y sea posible se individualizará en la resolución en función del grado de participación de cada responsable.

4. Las leyes reguladoras de los distintos regímenes sancionadores podrán tipificar como infracción el incumplimiento de la obligación de prevenir la comisión de infracciones administrativas por quienes se hallen sujetos a una relación de dependencia o vinculación. Asimismo, podrán prever los supuestos en que determinadas personas responderán del pago de las sanciones pecuniarias impuestas a quienes de ellas dependan o estén vinculadas.

Artículo 29. *Principio de proporcionalidad.*

1. Las sanciones administrativas, sean o no de naturaleza pecuniaria, en ningún caso podrán implicar, directa o subsidiariamente, privación de libertad.

2. El establecimiento de sanciones pecuniarias deberá prever que la comisión de las infracciones tipificadas no resulte más beneficioso para el infractor que el cumplimiento de las normas infringidas.

3. En la determinación normativa del régimen sancionador, así como en la imposición de sanciones por las Administraciones Públicas se deberá observar la debida idoneidad y

necesidad de la sanción a imponer y su adecuación a la gravedad del hecho constitutivo de la infracción. La graduación de la sanción considerará especialmente los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.
b) La continuidad o persistencia en la conducta infractora.
c) La naturaleza de los perjuicios causados.
d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

4. Cuando lo justifique la debida adecuación entre la sanción que deba aplicarse con la gravedad del hecho constitutivo de la infracción y las circunstancias concurrentes, el órgano competente para resolver podrá imponer la sanción en el grado inferior.

5. Cuando de la comisión de una infracción derive necesariamente la comisión de otra u otras, se deberá imponer únicamente la sanción correspondiente a la infracción más grave cometida.

6. Será sancionable, como infracción continuada, la realización de una pluralidad de acciones u omisiones que infrinjan el mismo o semejantes preceptos administrativos, en ejecución de un plan preconcebido o aprovechando idéntica ocasión.

Artículo 30. *Prescripción.*

1. Las infracciones y sanciones prescribirán según lo dispuesto en las leyes que las establezcan. Si éstas no fijan plazos de prescripción, las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

2. El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción se hubiera cometido. En el caso de infracciones continuadas o permanentes, el plazo comenzará a correr desde que finalizó la conducta infractora.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, de un procedimiento administrativo de naturaleza sancionadora, reiniciándose el plazo de prescripción si el expediente sancionador estuviera paralizado durante más de un mes por causa no imputable al presunto responsable.

3. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si aquél está paralizado durante más de un mes por causa no imputable al infractor.

En el caso de desestimación presunta del recurso de alzada interpuesto contra la resolución por la que se impone la sanción, el plazo de prescripción de la sanción comenzará a contarse desde el día siguiente a aquel en que finalice el plazo legalmente previsto para la resolución de dicho recurso.

Artículo 31. *Concurrencia de sanciones.*

1. No podrán sancionarse los hechos que lo hayan sido penal o administrativamente, en los casos en que se aprecie identidad del sujeto, hecho y fundamento.

2. Cuando un órgano de la Unión Europea hubiera impuesto una sanción por los mismos hechos, y siempre que no concurra la identidad de sujeto y fundamento, el órgano competente para resolver deberá tenerla en cuenta a efectos de graduar la que, en su caso, deba imponer, pudiendo minorarla, sin perjuicio de declarar la comisión de la infracción.

CAPÍTULO IV

De la responsabilidad patrimonial de las Administraciones Públicas

Sección 1.ª Responsabilidad patrimonial de las Administraciones Públicas

Artículo 32. *Principios de la responsabilidad.*

1. Los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos salvo en los casos de fuerza mayor o de daños que el particular tenga el deber jurídico de soportar de acuerdo con la Ley.

La anulación en vía administrativa o por el orden jurisdiccional contencioso administrativo de los actos o disposiciones administrativas no presupone, por sí misma, derecho a la indemnización.

2. En todo caso, el daño alegado habrá de ser efectivo, evaluable económicamente e individualizado con relación a una persona o grupo de personas.

3. Asimismo, los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas de toda lesión que sufran en sus bienes y derechos como consecuencia de la aplicación de actos legislativos de naturaleza no expropiatoria de derechos que no tengan el deber jurídico de soportar cuando así se establezca en los propios actos legislativos y en los términos que en ellos se especifiquen.

La responsabilidad del Estado legislador podrá surgir también en los siguientes supuestos, siempre que concurran los requisitos previstos en los apartados anteriores:

a) Cuando los daños deriven de la aplicación de una norma con rango de ley declarada inconstitucional, siempre que concurran los requisitos del apartado 4.

b) Cuando los daños deriven de la aplicación de una norma contraria al Derecho de la Unión Europea, de acuerdo con lo dispuesto en el apartado 5.

4. Si la lesión es consecuencia de la aplicación de una norma con rango de ley declarada inconstitucional, procederá su indemnización cuando el particular haya obtenido, en cualquier instancia, sentencia firme desestimatoria de un recurso contra la actuación administrativa que ocasionó el daño, siempre que se hubiera alegado la inconstitucionalidad posteriormente declarada.

5. Si la lesión es consecuencia de la aplicación de una norma declarada contraria al Derecho de la Unión Europea, procederá su indemnización cuando el particular haya obtenido, en cualquier instancia, sentencia firme desestimatoria de un recurso contra la actuación administrativa que ocasionó el daño, siempre que se hubiera alegado la infracción del Derecho de la Unión Europea posteriormente declarada. Asimismo, deberán cumplirse todos los requisitos siguientes:

a) La norma ha de tener por objeto conferir derechos a los particulares.

b) El incumplimiento ha de estar suficientemente caracterizado.

c) Ha de existir una relación de causalidad directa entre el incumplimiento de la obligación impuesta a la Administración responsable por el Derecho de la Unión Europea y el daño sufrido por los particulares.

6. La sentencia que declare la inconstitucionalidad de la norma con rango de ley o declare el carácter de norma contraria al Derecho de la Unión Europea producirá efectos desde la fecha de su publicación en el «Boletín Oficial del Estado» o en el «Diario Oficial de la Unión Europea», según el caso, salvo que en ella se establezca otra cosa.

7. La responsabilidad patrimonial del Estado por el funcionamiento de la Administración de Justicia se regirá por la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

8. El Consejo de Ministros fijará el importe de las indemnizaciones que proceda abonar cuando el Tribunal Constitucional haya declarado, a instancia de parte interesada, la existencia de un funcionamiento anormal en la tramitación de los recursos de amparo o de las cuestiones de inconstitucionalidad.

El procedimiento para fijar el importe de las indemnizaciones se tramitará por el Ministerio de Justicia, con audiencia al Consejo de Estado.

9. Se seguirá el procedimiento previsto en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas para determinar la responsabilidad de las Administraciones Públicas por los daños y perjuicios causados a terceros durante la ejecución de contratos cuando sean consecuencia de una orden inmediata y directa de la Administración o de los vicios del proyecto elaborado por ella misma sin perjuicio de las especialidades que, en su caso establezca el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

Artículo 33. *Responsabilidad concurrente de las Administraciones Públicas.*

1. Cuando de la gestión dimanante de fórmulas conjuntas de actuación entre varias Administraciones públicas se derive responsabilidad en los términos previstos en la presente Ley, las Administraciones intervinientes responderán frente al particular, en todo caso, de forma solidaria. El instrumento jurídico regulador de la actuación conjunta podrá determinar la distribución de la responsabilidad entre las diferentes Administraciones públicas.

2. En otros supuestos de concurrencia de varias Administraciones en la producción del daño, la responsabilidad se fijará para cada Administración atendiendo a los criterios de competencia, interés público tutelado e intensidad de la intervención. La responsabilidad será solidaria cuando no sea posible dicha determinación.

3. En los casos previstos en el apartado primero, la Administración competente para incoar, instruir y resolver los procedimientos en los que exista una responsabilidad concurrente de varias Administraciones Públicas, será la fijada en los Estatutos o reglas de la organización colegiada. En su defecto, la competencia vendrá atribuida a la Administración Pública con mayor participación en la financiación del servicio.

4. Cuando se trate de procedimientos en materia de responsabilidad patrimonial, la Administración Pública competente a la que se refiere el apartado anterior, deberá consultar a las restantes Administraciones implicadas para que, en el plazo de quince días, éstas puedan exponer cuanto consideren procedente.

Artículo 34. *Indemnización.*

1. Sólo serán indemnizables las lesiones producidas al particular provenientes de daños que éste no tenga el deber jurídico de soportar de acuerdo con la Ley. No serán indemnizables los daños que se deriven de hechos o circunstancias que no se hubiesen podido prever o evitar según el estado de los conocimientos de la ciencia o de la técnica existentes en el momento de producción de aquéllos, todo ello sin perjuicio de las prestaciones asistenciales o económicas que las leyes puedan establecer para estos casos.

En los casos de responsabilidad patrimonial a los que se refiere los apartados 4 y 5 del artículo 32, serán indemnizables los daños producidos en el plazo de los cinco años anteriores a la fecha de la publicación de la sentencia que declare la inconstitucionalidad de la norma con rango de ley o el carácter de norma contraria al Derecho de la Unión Europea, salvo que la sentencia disponga otra cosa.

2. La indemnización se calculará con arreglo a los criterios de valoración establecidos en la legislación fiscal, de expropiación forzosa y demás normas aplicables, ponderándose, en su caso, las valoraciones predominantes en el mercado. En los casos de muerte o lesiones corporales se podrá tomar como referencia la valoración incluida en los baremos de la normativa vigente en materia de Seguros obligatorios y de la Seguridad Social.

3. La cuantía de la indemnización se calculará con referencia al día en que la lesión efectivamente se produjo, sin perjuicio de su actualización a la fecha en que se ponga fin al procedimiento de responsabilidad con arreglo al Índice de Garantía de la Competitividad, fijado por el Instituto Nacional de Estadística, y de los intereses que procedan por demora en el pago de la indemnización fijada, los cuales se exigirán con arreglo a lo establecido en la Ley 47/2003, de 26 de noviembre, General Presupuestaria, o, en su caso, a las normas presupuestarias de las Comunidades Autónomas.

4. La indemnización procedente podrá sustituirse por una compensación en especie o ser abonada mediante pagos periódicos, cuando resulte más adecuado para lograr la reparación debida y convenga al interés público, siempre que exista acuerdo con el interesado.

Artículo 35. *Responsabilidad de Derecho Privado.*

Cuando las Administraciones Públicas actúen, directamente o a través de una entidad de derecho privado, en relaciones de esta naturaleza, su responsabilidad se exigirá de conformidad con lo previsto en los artículos 32 y siguientes, incluso cuando concurra con sujetos de derecho privado o la responsabilidad se exija directamente a la entidad de derecho privado a través de la cual actúe la Administración o a la entidad que cubra su responsabilidad.

Sección 2.ª Responsabilidad de las autoridades y personal al servicio de las Administraciones Públicas

Artículo 36. *Exigencia de la responsabilidad patrimonial de las autoridades y personal al servicio de las Administraciones Públicas.*

1. Para hacer efectiva la responsabilidad patrimonial a que se refiere esta Ley, los particulares exigirán directamente a la Administración Pública correspondiente las indemnizaciones por los daños y perjuicios causados por las autoridades y personal a su servicio.

2. La Administración correspondiente, cuando hubiere indemnizado a los lesionados, exigirá de oficio en vía administrativa de sus autoridades y demás personal a su servicio la responsabilidad en que hubieran incurrido por dolo, o culpa o negligencia graves, previa instrucción del correspondiente procedimiento.

Para la exigencia de dicha responsabilidad y, en su caso, para su cuantificación, se ponderarán, entre otros, los siguientes criterios: el resultado dañoso producido, el grado de culpabilidad, la responsabilidad profesional del personal al servicio de las Administraciones públicas y su relación con la producción del resultado dañoso.

3. Asimismo, la Administración instruirá igual procedimiento a las autoridades y demás personal a su servicio por los daños y perjuicios causados en sus bienes o derechos cuando hubiera concurrido dolo, o culpa o negligencia graves.

4. El procedimiento para la exigencia de la responsabilidad al que se refieren los apartados 2 y 3, se sustanciará conforme a lo dispuesto en la Ley de Procedimiento Administrativo Común de las Administraciones Públicas y se iniciará por acuerdo del órgano competente que se notificará a los interesados y que constará, al menos, de los siguientes trámites:

a) Alegaciones durante un plazo de quince días.

b) Práctica de las pruebas admitidas y cualesquiera otras que el órgano competente estime oportunas durante un plazo de quince días.

c) Audiencia durante un plazo de diez días.

d) Formulación de la propuesta de resolución en un plazo de cinco días a contar desde la finalización del trámite de audiencia.

e) Resolución por el órgano competente en el plazo de cinco días.

5. La resolución declaratoria de responsabilidad pondrá fin a la vía administrativa.

6. Lo dispuesto en los apartados anteriores, se entenderá sin perjuicio de pasar, si procede, el tanto de culpa a los Tribunales competentes.

Artículo 37. *Responsabilidad penal.*

1. La responsabilidad penal del personal al servicio de las Administraciones Públicas, así como la responsabilidad civil derivada del delito se exigirá de acuerdo con lo previsto en la legislación correspondiente.

2. La exigencia de responsabilidad penal del personal al servicio de las Administraciones Públicas no suspenderá los procedimientos de reconocimiento de responsabilidad patrimonial que se instruyan, salvo que la determinación de los hechos en el orden jurisdiccional penal sea necesaria para la fijación de la responsabilidad patrimonial.

CAPÍTULO V

Funcionamiento electrónico del sector público

Artículo 38. *La sede electrónica.*

1. La sede electrónica es aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias.

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.

3. Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad. En todo caso deberá garantizarse la identificación del órgano titular de la sede, así como los medios disponibles para la formulación de sugerencias y quejas.

4. Las sedes electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

5. La publicación en las sedes electrónicas de informaciones, servicios y transacciones respetará los principios de accesibilidad y uso de acuerdo con las normas establecidas al respecto, estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

6. Las sedes electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, certificados reconocidos o cualificados de autenticación de sitio web o medio equivalente.

Artículo 39. *Portal de internet.*

Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de Derecho Público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

Artículo 40. *Sistemas de identificación de las Administraciones Públicas.*

1. Las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

2. Se entenderá identificada la Administración Pública respecto de la información que se publique como propia en su portal de internet.

Artículo 41. *Actuación administrativa automatizada.*

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del

sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

Artículo 42. *Sistemas de firma para la actuación administrativa automatizada.*

En el ejercicio de la competencia en la actuación administrativa automatizada, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, basado en certificado electrónico reconocido o cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de Derecho Público, en los términos y condiciones establecidos, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

Artículo 43. *Firma electrónica del personal al servicio de las Administraciones Públicas.*

1. Sin perjuicio de lo previsto en los artículos 38, 41 y 42, la actuación de una Administración Pública, órgano, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano o empleado público.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios. Por razones de seguridad pública los sistemas de firma electrónica podrán referirse sólo el número de identificación profesional del empleado público.

Artículo 44. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, ésta determinará las condiciones y garantías por las que se regirá que, al menos, comprenderá la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Artículo 45. *Aseguramiento e interoperabilidad de la firma electrónica.*

1. Las Administraciones Públicas podrán determinar los trámites e informes que incluyan firma electrónica reconocida o cualificada y avanzada basada en certificados electrónicos reconocidos o cualificados de firma electrónica.

2. Con el fin de favorecer la interoperabilidad y posibilitar la verificación automática de la firma electrónica de los documentos electrónicos, cuando una Administración utilice sistemas de firma electrónica distintos de aquellos basados en certificado electrónico reconocido o cualificado, para remitir o poner a disposición de otros órganos, organismos públicos, entidades de Derecho Público o Administraciones la documentación firmada electrónicamente, podrá superponer un sello electrónico basado en un certificado electrónico reconocido o cualificado.

Artículo 46. *Archivo electrónico de documentos.*

1. Todos los documentos utilizados en las actuaciones administrativas se almacenarán por medios electrónicos, salvo cuando no sea posible.

2. Los documentos electrónicos que contengan actos administrativos que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados.

Artículo 46 bis. *Ubicación de los sistemas de información y comunicaciones para el registro de datos.*

Los sistemas de información y comunicaciones para la recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con tributos propios o cedidos y datos de los usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán ubicarse y prestarse dentro del territorio de la Unión Europea.

Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España.

CAPÍTULO VI

De los convenios

Artículo 47. *Definición y tipos de convenios.*

1. Son convenios los acuerdos con efectos jurídicos adoptados por las Administraciones Públicas, los organismos públicos y entidades de derecho público vinculados o dependientes o las Universidades públicas entre sí o con sujetos de derecho privado para un fin común.

No tienen la consideración de convenios, los Protocolos Generales de Actuación o instrumentos similares que comporten meras declaraciones de intención de contenido general o que expresen la voluntad de las Administraciones y partes suscriptoras para actuar con un objetivo común, siempre que no supongan la formalización de compromisos jurídicos concretos y exigibles.

Los convenios no podrán tener por objeto prestaciones propias de los contratos. En tal caso, su naturaleza y régimen jurídico se ajustará a lo previsto en la legislación de contratos del sector público.

2. Los convenios que suscriban las Administraciones Públicas, los organismos públicos y las entidades de derecho público vinculados o dependientes y las Universidades públicas, deberán corresponder a alguno de los siguientes tipos:

a) Convenios interadministrativos firmados entre dos o más Administraciones Públicas, o bien entre dos o más organismos públicos o entidades de derecho público vinculados o dependientes de distintas Administraciones públicas, y que podrán incluir la utilización de medios, servicios y recursos de otra Administración Pública, organismo público o entidad de derecho público vinculado o dependiente, para el ejercicio de competencias propias o delegadas.

Quedan excluidos los convenios interadministrativos suscritos entre dos o más Comunidades Autónomas para la gestión y prestación de servicios propios de las mismas, que se regirán en cuanto a sus supuestos, requisitos y términos por lo previsto en sus respectivos Estatutos de autonomía.

b) Convenios intradministrativos firmados entre organismos públicos y entidades de derecho público vinculados o dependientes de una misma Administración Pública.

c) Convenios firmados entre una Administración Pública u organismo o entidad de derecho público y un sujeto de Derecho privado.

d) Convenios no constitutivos ni de Tratado internacional, ni de Acuerdo internacional administrativo, ni de Acuerdo internacional no normativo, firmados entre las Administraciones Públicas y los órganos, organismos públicos o entes de un sujeto de Derecho internacional, que estarán sometidos al ordenamiento jurídico interno que determinen las partes.

Artículo 48. *Requisitos de validez y eficacia de los convenios.*

1. Las Administraciones Públicas, sus organismos públicos y entidades de derecho público vinculados o dependientes y las Universidades públicas, en el ámbito de sus respectivas competencias, podrán suscribir convenios con sujetos de derecho público y privado, sin que ello pueda suponer cesión de la titularidad de la competencia.

2. En el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, podrán celebrar convenios los titulares de los Departamentos Ministeriales y los Presidentes o Directores de las dichas entidades y organismos públicos.

3. La suscripción de convenios deberá mejorar la eficiencia de la gestión pública, facilitar la utilización conjunta de medios y servicios públicos, contribuir a la realización de actividades de utilidad pública y cumplir con la legislación de estabilidad presupuestaria y sostenibilidad financiera.

4. La gestión, justificación y resto de actuaciones relacionadas con los gastos derivados de los convenios que incluyan compromisos financieros para la Administración Pública o cualquiera de sus organismos públicos o entidades de derecho público vinculados o dependientes que lo suscriban, así como con los fondos comprometidos en virtud de dichos convenios, se ajustarán a lo dispuesto en la legislación presupuestaria.

5. Los convenios que incluyan compromisos financieros deberán ser financieramente sostenibles, debiendo quienes los suscriban tener capacidad para financiar los asumidos durante la vigencia del convenio.

6. Las aportaciones financieras que se comprometan a realizar los firmantes no podrán ser superiores a los gastos derivados de la ejecución del convenio.

7. Cuando el convenio instrumente una subvención deberá cumplir con lo previsto en la Ley 38/2003, de 17 de noviembre, General de Subvenciones y en la normativa autonómica de desarrollo que, en su caso, resulte aplicable.

Asimismo, cuando el convenio tenga por objeto la delegación de competencias en una Entidad Local, deberá cumplir con lo dispuesto en Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

8. Los convenios se perfeccionan por la prestación del consentimiento de las partes.

Los convenios suscritos por la Administración General del Estado o alguno de sus organismos públicos o entidades de derecho público vinculados o dependientes resultarán eficaces una vez inscritos, en el plazo de 5 días hábiles desde su formalización, en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación del sector público estatal, al que se refiere la disposición adicional séptima. Asimismo, serán publicados en el plazo de 10 días hábiles desde su formalización en el «Boletín Oficial del Estado», sin perjuicio de su publicación facultativa en el boletín oficial de la comunidad autónoma o de la provincia que corresponda a la otra administración firmante.

9. Las normas del presente Capítulo no serán de aplicación a las encomiendas de gestión y los acuerdos de terminación convencional de los procedimientos administrativos.

Artículo 49. *Contenido de los convenios.*

Los convenios a los que se refiere el apartado 1 del artículo anterior deberán incluir, al menos, las siguientes materias:

a) Sujetos que suscriben el convenio y la capacidad jurídica con que actúa cada una de las partes.

b) La competencia en la que se fundamenta la actuación de la Administración Pública, de los organismos públicos y las entidades de derecho público vinculados o dependientes de ella o de las Universidades públicas.

c) Objeto del convenio y actuaciones a realizar por cada sujeto para su cumplimiento, indicando, en su caso, la titularidad de los resultados obtenidos.

d) Obligaciones y compromisos económicos asumidos por cada una de las partes, si los hubiera, indicando su distribución temporal por anualidades y su imputación concreta al presupuesto correspondiente de acuerdo con lo previsto en la legislación presupuestaria.

e) Consecuencias aplicables en caso de incumplimiento de las obligaciones y compromisos asumidos por cada una de las partes y, en su caso, los criterios para determinar la posible indemnización por el incumplimiento.

f) Mecanismos de seguimiento, vigilancia y control de la ejecución del convenio y de los compromisos adquiridos por los firmantes. Este mecanismo resolverá los problemas de interpretación y cumplimiento que puedan plantearse respecto de los convenios.

g) El régimen de modificación del convenio. A falta de regulación expresa la modificación del contenido del convenio requerirá acuerdo unánime de los firmantes.

h) Plazo de vigencia del convenio teniendo en cuenta las siguientes reglas:

1.º Los convenios deberán tener una duración determinada, que no podrá ser superior a cuatro años, salvo que normativamente se prevea un plazo superior.

2.º En cualquier momento antes de la finalización del plazo previsto en el apartado anterior, los firmantes del convenio podrán acordar unánimemente su prórroga por un periodo de hasta cuatro años adicionales o su extinción.

En el caso de convenios suscritos por la Administración General del Estado o alguno de sus organismos públicos y entidades de derecho público vinculados o dependientes, esta prórroga deberá ser comunicada al Registro Electrónico estatal de Órganos e Instrumentos de Cooperación al que se refiere la disposición adicional séptima.

Artículo 50. *Trámites preceptivos para la suscripción de convenios y sus efectos.*

1. Sin perjuicio de las especialidades que la legislación autonómica pueda prever, será necesario que el convenio se acompañe de una memoria justificativa donde se analice su necesidad y oportunidad, su impacto económico, el carácter no contractual de la actividad en cuestión, así como el cumplimiento de lo previsto en esta Ley.

2. Los convenios que suscriba la Administración General del Estado o sus organismos públicos y entidades de derecho público vinculados o dependientes se acompañarán además de:

a) El informe de su servicio jurídico, que deberá emitirse en un plazo máximo de siete días hábiles desde su solicitud, transcurridos los cuales se continuará la tramitación. En todo/ caso, dicho informe deberá emitirse e incorporarse al expediente antes de proceder al perfeccionamiento del convenio. No será necesario solicitar este informe cuando el convenio se ajuste a un modelo normalizado informado previamente por el servicio jurídico que corresponda.

b) Cualquier otro informe preceptivo que establezca la normativa aplicable, que deberá emitirse en un plazo máximo de siete días hábiles desde su solicitud, transcurridos los cuales se continuará la tramitación. En cualquier caso, deberán emitirse e incorporarse al expediente todos los informes preceptivos antes de proceder al perfeccionamiento del convenio.

c) La autorización previa del Ministerio de Hacienda y Función Pública para su firma, modificación, prórroga y resolución por mutuo acuerdo entre las partes, que deberá emitirse en un plazo máximo de siete días hábiles desde la solicitud, transcurridos los cuales se continuará la tramitación. En todo caso dicha autorización deberá emitirse e incorporarse al expediente antes de proceder al perfeccionamiento del convenio.

Cuando el convenio a suscribir esté excepcionado de la autorización a la que se refiere el párrafo anterior, también lo estará del informe del Ministerio de Política Territorial.

No obstante, en todo caso, será preceptivo el informe del Ministerio de Política Territorial, respecto de los convenios que se suscriban entre la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, con las Comunidades Autónomas o con Entidades Locales o con sus organismos públicos y entidades de derecho público vinculados o dependientes, en los casos siguientes:

1. Convenios cuyo objeto sea la cesión o adquisición de la titularidad de infraestructuras por la Administración General del Estado.
2. Convenios que tengan por objeto la creación de consorcios previstos en el artículo 123 de esta ley.

d) Cuando los convenios plurianuales suscritos entre Administraciones Públicas incluyan aportaciones de fondos por parte del Estado para financiar actuaciones a ejecutar exclusivamente por parte de otra Administración Pública y el Estado asuma, en el ámbito de sus competencias, los compromisos frente a terceros, la aportación del Estado de anualidades futuras estará condicionada a la existencia de crédito en los correspondientes presupuestos.
e) Los convenios interadministrativos suscritos con las Comunidades Autónomas serán remitidos al Senado por el Ministerio de Política Territorial.

Artículo 51. *Extinción de los convenios.*

1. Los convenios se extinguen por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en causa de resolución.
2. Son causas de resolución:

a) El transcurso del plazo de vigencia del convenio sin haberse acordado la prórroga del mismo.
b) El acuerdo unánime de todos los firmantes.
c) El incumplimiento de las obligaciones y compromisos asumidos por parte de alguno de los firmantes.
En este caso, cualquiera de las partes podrá notificar a la parte incumplidora un requerimiento para que cumpla en un determinado plazo con las obligaciones o compromisos que se consideran incumplidos. Este requerimiento será comunicado al responsable del mecanismo de seguimiento, vigilancia y control de la ejecución del convenio y a las demás partes firmantes.
Si trascurrido el plazo indicado en el requerimiento persistiera el incumplimiento, la parte que lo dirigió notificará a las partes firmantes la concurrencia de la causa de resolución y se entenderá resuelto el convenio. La resolución del convenio por esta causa podrá conllevar la indemnización de los perjuicios causados si así se hubiera previsto.
d) Por decisión judicial declaratoria de la nulidad del convenio.
e) Por cualquier otra causa distinta de las anteriores prevista en el convenio o en otras leyes.

Artículo 52. *Efectos de la resolución de los convenios.*

1. El cumplimiento y la resolución de los convenios dará lugar a la liquidación de los mismos con el objeto de determinar las obligaciones y compromisos de cada una de las partes.
2. En el supuesto de convenios de los que deriven compromisos financieros, se entenderán cumplidos cuando su objeto se haya realizado en los términos y a satisfacción de ambas partes, de acuerdo con sus respectivas competencias, teniendo en cuenta las siguientes reglas:

a) Si de la liquidación resultara que el importe de las actuaciones ejecutadas por alguna de las partes fuera inferior a los fondos que la misma hubiera recibido del resto de partes del convenio para financiar dicha ejecución, aquella deberá reintegrar a estas el exceso que corresponda a cada una, **en el plazo máximo de un mes desde que se hubiera aprobado la liquidación.**
Transcurrido el plazo máximo de un mes, mencionado en el párrafo anterior, sin que se haya producido el reintegro, se deberá abonar a dichas partes, **también en el plazo**

de un mes a contar desde ese momento, el interés de demora aplicable al citado reintegro, que será en todo caso el que resulte de las disposiciones de carácter general reguladoras del gasto público y de la actividad económico-financiera del sector público.

b) Si fuera superior, el resto de partes del convenio, **en el plazo de un mes desde la aprobación de la liquidación**, deberá abonar a la parte de que se trate la diferencia que corresponda a cada una de ellas, con el límite máximo de las cantidades que cada una de ellas se hubiera comprometido a aportar en virtud del convenio. En ningún caso las partes del convenio tendrán derecho a exigir al resto cuantía alguna que supere los citados límites máximos.

Téngase en cuenta que se declaran contrarios al orden constitucional de competencias, en los términos del fundamento jurídico 8.b), los incisos destacados del apartado 2, por Sentencia del TC 132/2018, de 13 de diciembre. Ref. BOE-A-2019-457

3. No obstante lo anterior, si cuando concurra cualquiera de las causas de resolución del convenio existen actuaciones en curso de ejecución, las partes, a propuesta de la comisión de seguimiento, vigilancia y control del convenio o, en su defecto, del responsable del mecanismo a que hace referencia la letra f) del artículo 49, podrán acordar la continuación y finalización de las actuaciones en curso que consideren oportunas, estableciendo un plazo improrrogable para su finalización, transcurrido el cual deberá realizarse la liquidación de las mismas en los términos establecidos en el apartado anterior.

Artículo 53. *Remisión de convenios al Tribunal de Cuentas.*

1. Dentro de los tres meses siguientes a la suscripción de cualquier convenio cuyos compromisos económicos asumidos superen los 600.000 euros, estos deberán remitirse electrónicamente al Tribunal de Cuentas u órgano externo de fiscalización de la Comunidad Autónoma, según corresponda.

2. Igualmente se comunicarán al Tribunal de Cuentas u órgano externo de fiscalización de la Comunidad Autónoma, según corresponda, las modificaciones, prórrogas o variaciones de plazos, alteración de los importes de los compromisos económicos asumidos y la extinción de los convenios indicados.

3. Lo dispuesto en los apartados anteriores se entenderá sin perjuicio de las facultades del Tribunal de Cuentas o, en su caso, de los correspondientes órganos de fiscalización externos de las Comunidades Autónomas, para reclamar cuantos datos, documentos y antecedentes estime pertinentes con relación a los contratos de cualquier naturaleza y cuantía.

TÍTULO I

Administración General del Estado

CAPÍTULO I

Organización administrativa

Artículo 54. *Principios y competencias de organización y funcionamiento de la Administración General del Estado.*

1. La Administración General del Estado actúa y se organiza de acuerdo con los principios establecidos en el artículo 3, así como los de descentralización funcional y desconcentración funcional y territorial.

2. Las competencias en materia de organización administrativa, régimen de personal, procedimientos e inspección de servicios, no atribuidas específicamente conforme a una Ley a ningún otro órgano de la Administración General del Estado, ni al Gobierno, corresponderán al Ministerio de Hacienda y Administraciones Públicas.

Artículo 55. *Estructura de la Administración General del Estado.*

1. La organización de la Administración General del Estado responde a los principios de división funcional en Departamentos ministeriales y de gestión territorial integrada en Delegaciones del Gobierno en las Comunidades Autónomas, salvo las excepciones previstas por esta Ley.

2. La Administración General del Estado comprende:

a) La Organización Central, que integra los Ministerios y los servicios comunes.
b) La Organización Territorial.
c) La Administración General del Estado en el exterior.

3. En la organización central son órganos superiores y órganos directivos:

a) Órganos superiores:

1.º Los Ministros.
2.º Los Secretarios de Estado.

b) Órganos directivos:

1.º Los Subsecretarios y Secretarios generales.
2.º Los Secretarios generales técnicos y Directores generales.
3.º Los Subdirectores generales.

4. En la organización territorial de la Administración General del Estado son órganos directivos tanto los Delegados del Gobierno en las Comunidades Autónomas, que tendrán rango de Subsecretario, como los Subdelegados del Gobierno en las provincias, los cuales tendrán nivel de Subdirector general.

5. En la Administración General del Estado en el exterior son órganos directivos los embajadores y representantes permanentes ante Organizaciones internacionales.

6. Los órganos superiores y directivos tienen además la condición de alto cargo, excepto los Subdirectores generales y asimilados, de acuerdo con lo previsto en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

7. Todos los demás órganos de la Administración General del Estado se encuentran bajo la dependencia o dirección de un órgano superior o directivo.

8. Los estatutos de los Organismos públicos determinarán sus respectivos órganos directivos.

9. Corresponde a los órganos superiores establecer los planes de actuación de la organización situada bajo su responsabilidad y a los órganos directivos su desarrollo y ejecución.

10. Los Ministros y Secretarios de Estado son nombrados de acuerdo con lo establecido en la Ley 50/1997, de 27 de noviembre, del Gobierno y en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

11. Sin perjuicio de lo previsto en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, los titulares de los órganos superiores y directivos son nombrados, atendiendo a criterios de competencia profesional y experiencia, en la forma establecida en esta Ley, siendo de aplicación al desempeño de sus funciones:

a) La responsabilidad profesional, personal y directa por la gestión desarrollada.
b) La sujeción al control y evaluación de la gestión por el órgano superior o directivo competente, sin perjuicio del control establecido por la Ley General Presupuestaria.

Artículo 56. *Elementos organizativos básicos.*

1. Las unidades administrativas son los elementos organizativos básicos de las estructuras orgánicas. Las unidades comprenden puestos de trabajo o dotaciones de plantilla vinculados funcionalmente por razón de sus cometidos y orgánicamente por una jefatura común. Pueden existir unidades administrativas complejas, que agrupen dos o más unidades menores.

2. Los jefes de las unidades administrativas son responsables del correcto funcionamiento de la unidad y de la adecuada ejecución de las tareas asignadas a la misma.

3. Las unidades administrativas se establecen mediante las relaciones de puestos de trabajo, que se aprobarán de acuerdo con su regulación específica, y se integran en un determinado órgano.

CAPÍTULO II

Los Ministerios y su estructura interna

Artículo 57. *Los Ministerios.*

1. La Administración General del Estado se organiza en Presidencia del Gobierno y en Ministerios, comprendiendo a cada uno de ellos uno o varios sectores funcionalmente homogéneos de actividad administrativa.

2. La organización en Departamentos ministeriales no obsta a la existencia de órganos superiores o directivos u Organismos públicos no integrados o dependientes, respectivamente, en la estructura general del Ministerio que con carácter excepcional se adscriban directamente al Ministro.

3. La determinación del número, la denominación y el ámbito de competencia respectivo de los Ministerios y las Secretarías de Estado se establecen mediante Real Decreto del Presidente del Gobierno.

Artículo 58. *Organización interna de los Ministerios.*

1. En los Ministerios pueden existir Secretarías de Estado, y Secretarías Generales, para la gestión de un sector de actividad administrativa. De ellas dependerán jerárquicamente los órganos directivos que se les adscriban.

2. Los Ministerios contarán, en todo caso, con una Subsecretaría, y dependiendo de ella una Secretaría General Técnica, para la gestión de los servicios comunes previstos en este Título.

3. Las Direcciones Generales son los órganos de gestión de una o varias áreas funcionalmente homogéneas.

4. Las Direcciones Generales se organizan en Subdirecciones Generales para la distribución de las competencias encomendadas a aquéllas, la realización de las actividades que les son propias y la asignación de objetivos y responsabilidades. Sin perjuicio de lo anterior, podrán adscribirse directamente Subdirecciones Generales a otros órganos directivos de mayor nivel o a órganos superiores del Ministerio.

Artículo 59. *Creación, modificación y supresión de órganos y unidades administrativas.*

1. Las Subsecretarías, las Secretarías Generales, las Secretarías Generales Técnicas, las Direcciones Generales, las Subdirecciones Generales, y órganos similares a los anteriores se crean, modifican y suprimen por Real Decreto del Consejo de Ministros, a iniciativa del Ministro interesado y a propuesta del Ministro de Hacienda y Administraciones Públicas.

2. Los órganos de nivel inferior a Subdirección General se crean, modifican y suprimen por orden del Ministro respectivo, previa autorización del Ministro de Hacienda y Administraciones Públicas.

3. Las unidades que no tengan la consideración de órganos se crean, modifican y suprimen a través de las relaciones de puestos de trabajo.

Artículo 60. *Ordenación jerárquica de los órganos ministeriales.*

1. Los Ministros son los jefes superiores del Departamento y superiores jerárquicos directos de los Secretarios de Estado y Subsecretarios.

2. Los órganos directivos dependen de alguno de los anteriores y se ordenan jerárquicamente entre sí de la siguiente forma: Subsecretario, Director general y Subdirector general.

Los Secretarios generales tienen categoría de Subsecretario y los Secretarios Generales Técnicos tienen categoría de Director general.

Artículo 61. *Los Ministros.*

Los Ministros, como titulares del departamento sobre el que ejercen su competencia, dirigen los sectores de actividad administrativa integrados en su Ministerio, y asumen la responsabilidad inherente a dicha dirección. A tal fin, les corresponden las siguientes funciones:

a) Ejercer la potestad reglamentaria en las materias propias de su Departamento.

b) Fijar los objetivos del Ministerio, aprobar los planes de actuación del mismo y asignar los recursos necesarios para su ejecución, dentro de los límites de las dotaciones presupuestarias correspondientes.

c) Aprobar las propuestas de los estados de gastos del Ministerio, y de los presupuestos de los Organismos públicos dependientes y remitirlas al Ministerio de Hacienda y Administraciones Públicas.

d) Determinar y, en su caso, proponer la organización interna de su Ministerio, de acuerdo con las competencias que le atribuye esta Ley.

e) Evaluar la realización de los planes de actuación del Ministerio por parte de los órganos superiores y órganos directivos y ejercer el control de eficacia respecto de la actuación de dichos órganos y de los Organismos públicos dependientes, sin perjuicio de lo dispuesto en la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

f) Nombrar y separar a los titulares de los órganos directivos del Ministerio y de los Organismos públicos o entidades de derecho público dependientes del mismo, cuando la competencia no esté atribuida al Consejo de Ministros a otro órgano o al propio organismo, así como elevar a aquél las propuestas de nombramientos que le estén reservadas de órganos directivos del Ministerio y de los Organismos Públicos dependientes del mismo.

g) Autorizar las comisiones de servicio con derecho a indemnización por cuantía exacta para altos cargos dependientes del Ministro.

h) Mantener las relaciones con las Comunidades Autónomas y convocar las Conferencias sectoriales y los órganos de cooperación en el ámbito de las competencias atribuidas a su Departamento.

i) Dirigir la actuación de los titulares de los órganos superiores y directivos del Ministerio, impartirles instrucciones concretas y delegarles competencias propias.

j) Revisar de oficio los actos administrativos y resolver los conflictos de atribuciones cuando les corresponda, así como plantear los que procedan con otros Ministerios.

k) Celebrar en el ámbito de su competencia, contratos y convenios, sin perjuicio de la autorización del Consejo de Ministros cuando sea preceptiva.

l) Administrar los créditos para gastos de los presupuestos del Ministerio, aprobar y comprometer los gastos que no sean de la competencia del Consejo de Ministros, aprobar las modificaciones presupuestarias que sean de su competencia, reconocer las obligaciones económicas y proponer su pago en el marco del plan de disposición de fondos del Tesoro Público, así como fijar los límites por debajo de los cuales estas competencias corresponderán, en su ámbito respectivo, a los Secretarios de Estado y Subsecretario del departamento. Corresponderá al Ministro elevar al Consejo de Ministros, para su aprobación, las modificaciones presupuestarias que sean de la competencia de éste.

m) Decidir la representación del Ministerio en los órganos colegiados o grupos de trabajo en los que no esté previamente determinado el titular del órgano superior o directivo que deba representar al Departamento.

n) Remitir la documentación a su Departamento necesaria para la elaboración de la Cuenta General del Estado, en los términos previstos en la Ley 47/2003, 26 de noviembre.

ñ) Resolver de los recursos administrativos y declarar la lesividad de los actos administrativos cuando les corresponda.

o) Otorgar premios y recompensas propios del Departamento y proponer las que corresponda según sus normas reguladoras.

p) Conceder subvenciones y ayudas con cargo a los créditos de gasto propios del Departamento, así como fijar los límites por debajo de los cuales podrán ser otorgadas por los Secretarios de Estado o el Subsecretario del Departamento.

q) Proponer y ejecutar, en el ámbito de su competencia, los Planes de Empleo del Departamento y de los organismos públicos de él dependientes.

r) Modificar las Relaciones de Puestos de Trabajo en los casos en que esa competencia esté delegada en el propio departamento o proponer al Ministerio de Hacienda y Administraciones Públicas las que sean de competencia de este último.

s) Imponer la sanción de separación del servicio por faltas muy graves.

t) Ejercer cuantas otras competencias les atribuyan las leyes, las normas de organización y funcionamiento del Gobierno y cualesquiera otras disposiciones.

Artículo 62. *Los Secretarios de Estado.*

1. Los Secretarios de Estado son directamente responsables de la ejecución de la acción del Gobierno en un sector de actividad específica.

Asimismo, podrán ostentar por delegación expresa de sus respectivos Ministros la representación de estos en materias propias de su competencia, incluidas aquellas con proyección internacional, sin perjuicio, en todo caso, de las normas que rigen las relaciones de España con otros Estados y con las Organizaciones internacionales.

2. Los Secretarios de Estado dirigen y coordinan las Secretarías y las Direcciones Generales situadas bajo su dependencia, y responden ante el Ministro de la ejecución de los objetivos fijados para la Secretaría de Estado. A tal fin les corresponde:

a) Ejercer las competencias sobre el sector de actividad administrativa asignado que les atribuya la norma de creación del órgano o que les delegue el Ministro y desempeñar las relaciones externas de la Secretaría de Estado, salvo en los casos legalmente reservados al Ministro.

b) Ejercer las competencias inherentes a su responsabilidad de dirección y, en particular, impulsar la consecución de los objetivos y la ejecución de los proyectos de su organización, controlando su cumplimiento, supervisando la actividad de los órganos directivos adscritos e impartiendo instrucciones a sus titulares.

c) Nombrar y separar a los Subdirectores Generales de la Secretaría de Estado.

d) Mantener las relaciones con los órganos de las Comunidades Autónomas competentes por razón de la materia.

e) La autorización previa para contratar a los Organismos Autónomos adscritos a la Secretaría de Estado, por encima de una cuantía determinada, según lo previsto en la disposición transitoria tercera del Real Decreto Legislativo 3/2011, de 14 de noviembre por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público.

f) Autorizar las comisiones de servicio con derecho a indemnización por cuantía exacta para los altos cargos dependientes de la Secretaría de Estado.

g) Celebrar contratos relativos a asuntos de su Secretaría de Estado y los convenios no reservados al Ministro del que dependan, sin perjuicio de la correspondiente autorización cuando sea preceptiva.

h) Conceder subvenciones y ayudas con cargo a los créditos de gasto propios de la Secretaría de Estado, con los límites establecidos por el titular del Departamento.

i) Resolver los recursos que se interpongan contra las resoluciones de los órganos directivos que dependan directamente de él y cuyos actos no agoten la vía administrativa, así como los conflictos de atribuciones que se susciten entre dichos órganos.

j) Administrar los créditos para gastos de los presupuestos del Ministerio por su materia propios de la Secretaría de Estado, aprobar las modificaciones presupuestarias de los mismos, aprobar y comprometer los gastos con cargo a aquellos créditos y reconocer las obligaciones económicas y proponer su pago en el marco del plan de disposición de fondos del Tesoro Público. Todo ello dentro de la cuantía que, en su caso, establezca el Ministro al efecto y siempre que los referidos actos no sean competencia del Consejo de Ministros.

k) Cualesquiera otras competencias que les atribuya la legislación en vigor.

Artículo 63. *Los Subsecretarios.*

1. Los Subsecretarios ostentan la representación ordinaria del Ministerio, dirigen los servicios comunes, ejercen las competencias correspondientes a dichos servicios comunes y, en todo caso, las siguientes:

a) Apoyar a los órganos superiores en la planificación de la actividad del Ministerio, a través del correspondiente asesoramiento técnico.

b) Asistir al Ministro en el control de eficacia del Ministerio y sus Organismos públicos.

c) Establecer los programas de inspección de los servicios del Ministerio, así como determinar las actuaciones precisas para la mejora de los sistemas de planificación, dirección y organización y para la racionalización y simplificación de los procedimientos y métodos de trabajo, en el marco definido por el Ministerio de Hacienda y Administraciones Públicas.

d) Proponer las medidas de organización del Ministerio y dirigir el funcionamiento de los servicios comunes a través de las correspondientes instrucciones u órdenes de servicio.

e) Asistir a los órganos superiores en materia de relaciones de puestos de trabajo, planes de empleo y política de directivos del Ministerio y sus Organismos públicos, así como en la elaboración, ejecución y seguimiento de los presupuestos y la planificación de los sistemas de información y comunicación.

f) Desempeñar la jefatura superior de todo el personal del Departamento.

g) Responsabilizarse del asesoramiento jurídico al Ministro en el desarrollo de las funciones que a éste le corresponden y, en particular, en el ejercicio de su potestad normativa y en la producción de los actos administrativos de la competencia de aquél, así como a los demás órganos del Ministerio.

En los mismos términos del párrafo anterior, informar las propuestas o proyectos de normas y actos de otros Ministerios, cuando reglamentariamente proceda.

A tales efectos, el Subsecretario será responsable de coordinar las actuaciones correspondientes dentro del Ministerio y en relación con los demás Ministerios que hayan de intervenir en el procedimiento.

h) Ejercer las facultades de dirección, impulso y supervisión de la Secretaría General Técnica y los restantes órganos directivos que dependan directamente de él.

i) Administrar los créditos para gastos de los presupuestos del Ministerio por su materia propios de la Subsecretaría, aprobar las modificaciones presupuestarias de los mismos, aprobar y comprometer los gastos con cargo a aquellos créditos y reconocer las obligaciones económicas y proponer su pago en el marco del plan de disposición de fondos del Tesoro Público. Todo ello dentro de la cuantía que, en su caso, establezca el Ministro al efecto y siempre que los referidos actos no sean competencia del Consejo de Ministros.

j) Conceder subvenciones y ayudas con cargo a los créditos de gasto propios del Ministerio con los límites establecidos por el titular del Departamento.

k) Solicitar del Ministerio de Hacienda y Administraciones Públicas la afectación o el arrendamiento de los inmuebles necesarios para el cumplimiento de los fines de los servicios a cargo del Departamento.

l) Nombrar y cesar a los Subdirectores y asimilados dependientes de la Subsecretaría, al resto de personal de libre designación y al personal eventual del Departamento.

m) Convocar y resolver pruebas selectivas de personal funcionario y laboral.

n) Convocar y resolver los concursos de personal funcionario.

ñ) Ejercer la potestad disciplinaria del personal del Departamento por faltas graves o muy graves, salvo la separación del servicio.

o) Adoptar e impulsar, bajo la dirección del Ministro, las medidas tendentes a la gestión centralizada de recursos humanos y medios materiales en el ámbito de su Departamento Ministerial.

p) Autorizar las comisiones de servicio con derecho a indemnización por cuantía exacta para altos cargos dependientes del Subsecretario.

q) Cualesquiera otras que sean inherentes a los servicios comunes del Ministerio y a la representación ordinaria del mismo y las que les atribuyan la legislación en vigor.

2. La Subsecretaría del Ministerio de la Presidencia, en coordinación con la Secretaría General de la Presidencia del Gobierno, ejercerá las competencias propias de los servicios comunes de los Departamentos en relación con el área de la Presidencia del Gobierno.

3. Los Subsecretarios serán nombrados y separados por Real Decreto del Consejo de Ministros a propuesta del titular del Ministerio.

Los nombramientos habrán de efectuarse entre funcionarios de carrera del Estado, de las Comunidades Autónomas o de las Entidades locales, pertenecientes al Subgrupo A1, a que se refiere el artículo 76 de la Ley 7/2007, de 12 de abril, por el que se aprueba el Estatuto Básico del Empleado Público. En todo caso, habrán de reunir los requisitos de

idoneidad establecidos en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

Artículo 64. *Los Secretarios generales.*

1. Cuando las normas que regulan la estructura de un Ministerio prevean la existencia de un Secretario general, deberán determinar las competencias que le correspondan sobre un sector de actividad administrativa determinado.

2. Los Secretarios generales ejercen las competencias inherentes a su responsabilidad de dirección sobre los órganos dependientes, contempladas en el artículo 62.2.b), así como todas aquellas que les asigne expresamente el Real Decreto de estructura del Ministerio.

3. Los Secretarios generales, con categoría de Subsecretario, serán nombrados y separados por Real Decreto del Consejo de Ministros, a propuesta del titular del Ministerio o del Presidente del Gobierno.

Los nombramientos habrán de efectuarse entre personas con cualificación y experiencia en el desempeño de puestos de responsabilidad en la gestión pública o privada. En todo caso, habrán de reunir los requisitos de idoneidad establecidos en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

Artículo 65. *Los Secretarios generales técnicos.*

1. Los Secretarios generales técnicos, bajo la inmediata dependencia del Subsecretario, tendrán las competencias sobre servicios comunes que les atribuya el Real Decreto de estructura del Departamento y, en todo caso, las relativas a producción normativa, asistencia jurídica y publicaciones.

2. Los Secretarios generales técnicos tienen a todos los efectos la categoría de Director General y ejercen sobre sus órganos dependientes las facultades atribuidas a dicho órgano por el artículo siguiente.

3. Los Secretarios generales técnicos serán nombrados y separados por Real Decreto del Consejo de Ministros a propuesta del titular del Ministerio.

Los nombramientos habrán de efectuarse entre funcionarios de carrera del Estado, de las Comunidades Autónomas o de las Entidades locales, pertenecientes al Subgrupo A1, a que se refiere el artículo 76 de la Ley 7/2007, de 12 de abril. En todo caso, habrán de reunir los requisitos de idoneidad establecidos en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio de alto cargo de la Administración General del Estado.

Artículo 66. *Los Directores generales.*

1. Los Directores generales son los titulares de los órganos directivos encargados de la gestión de una o varias áreas funcionalmente homogéneas del Ministerio. A tal efecto, les corresponde:

a) Proponer los proyectos de su Dirección general para alcanzar los objetivos establecidos por el Ministro, dirigir su ejecución y controlar su adecuado cumplimiento.

b) Ejercer las competencias atribuidas a la Dirección general y las que le sean desconcentradas o delegadas.

c) Proponer, en los restantes casos, al Ministro o al titular del órgano del que dependa, la resolución que estime procedente sobre los asuntos que afectan al órgano directivo.

d) Impulsar y supervisar las actividades que forman parte de la gestión ordinaria del órgano directivo y velar por el buen funcionamiento de los órganos y unidades dependientes y del personal integrado en los mismos.

e) Las demás atribuciones que le confieran las leyes y reglamentos.

2. Los Directores generales serán nombrados y separados por Real Decreto del Consejo de Ministros, a propuesta del titular del Departamento o del Presidente del Gobierno.

Los nombramientos habrán de efectuarse entre funcionarios de carrera del Estado, de las Comunidades Autónomas o de las Entidades locales, pertenecientes al Subgrupo A1, a que se refiere el artículo 76 de la Ley 7/2007, de 12 de abril, salvo que el Real Decreto de estructura permita que, en atención a las características específicas de las funciones de la Dirección General, su titular no reúna dicha condición de funcionario, debiendo motivarse

mediante memoria razonada la concurrencia de las especiales características que justifiquen esa circunstancia excepcional. En todo caso, habrán de reunir los requisitos de idoneidad establecidos en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

Artículo 67. *Los Subdirectores generales.*

1. Los Subdirectores generales son los responsables inmediatos, bajo la supervisión del Director general o del titular del órgano del que dependan, de la ejecución de aquellos proyectos, objetivos o actividades que les sean asignados, así como de la gestión ordinaria de los asuntos de la competencia de la Subdirección General.

2. Los Subdirectores generales serán nombrados, respetando los principios de igualdad, mérito y capacidad, y cesados por el Ministro, Secretario de Estado o Subsecretario del que dependan.

Los nombramientos habrán de efectuarse entre funcionarios de carrera del Estado, o de otras Administraciones, cuando así lo prevean las normas de aplicación, pertenecientes al Subgrupo A1, a que se refiere el artículo 76 de la Ley 7/2007, de 12 de abril.

Artículo 68. *Reglas generales sobre los servicios comunes de los Ministerios.*

1. Los órganos directivos encargados de los servicios comunes, prestan a los órganos superiores y directivos del resto del Ministerio la asistencia precisa para el más eficaz cumplimiento de sus cometidos y, en particular, la eficiente utilización de los medios y recursos materiales, económicos y personales que tengan asignados.

Corresponde a los servicios comunes el asesoramiento, el apoyo técnico y, en su caso, la gestión directa en relación con las funciones de planificación, programación y presupuestación, cooperación internacional, acción en el exterior, organización y recursos humanos, sistemas de información y comunicación, producción normativa, asistencia jurídica, gestión financiera, gestión de medios materiales y servicios auxiliares, seguimiento, control e inspección de servicios, estadística para fines estatales y publicaciones.

2. Los servicios comunes funcionan en cada Departamento de acuerdo con las disposiciones y directrices adoptadas por los Ministerios con competencia sobre dichas funciones comunes en la Administración General del Estado. Todo ello, sin perjuicio de que determinados órganos con competencia sobre algunos servicios comunes sigan dependiendo funcional o jerárquicamente de alguno de los referidos Ministerios.

3. Mediante Real Decreto podrá preverse la gestión compartida de algunos de los servicios comunes que podrá realizarse de las formas siguientes:

a) Mediante su coordinación directa por el Ministerio de Hacienda y Administraciones Públicas o por un organismo autónomo vinculado o dependiente del mismo, que prestarán algunos de estos servicios comunes a otros Ministerios.

b) Mediante su coordinación directa por la Subsecretaría de cada Ministerio o por un organismo autónomo vinculado o dependiente de la misma que prestará algunos de estos servicios comunes a todo el Ministerio. El Real Decreto que determine la gestión compartida de algunos de los servicios comunes concretará el régimen de dependencia orgánica y funcional del personal que viniera prestando el servicio respectivo en cada unidad.

CAPÍTULO III

Órganos territoriales

Sección 1.ª La organización territorial de la Administración General del Estado

Artículo 69. *Las Delegaciones y las Subdelegaciones del Gobierno.*

1. Existirá una Delegación del Gobierno en cada una de las Comunidades Autónomas.

2. Las Delegaciones del Gobierno tendrán su sede en la localidad donde radique el Consejo de Gobierno de la Comunidad Autónoma, salvo que el Consejo de Ministros acuerde ubicarla en otra distinta y sin perjuicio de lo que disponga expresamente el Estatuto de Autonomía.

3. Las Delegaciones del Gobierno están adscritas orgánicamente al Ministerio de Hacienda y Administraciones Públicas.

4. En cada una de las provincias de las Comunidades Autónomas pluriprovinciales, existirá un Subdelegado del Gobierno, que estará bajo la inmediata dependencia del Delegado del Gobierno.

Podrán crearse por Real Decreto Subdelegaciones del Gobierno en las Comunidades Autónomas uniprovinciales, cuando circunstancias tales como la población del territorio, el volumen de gestión o sus singularidades geográficas, sociales o económicas así lo justifiquen.

Artículo 70. *Los Directores Insulares de la Administración General del Estado.*

Reglamentariamente se determinarán las islas en las que existirá un Director Insular de la Administración General del Estado, con el nivel que se determine en la relación de puestos de trabajo. Serán nombrados por el Delegado del Gobierno mediante el procedimiento de libre designación entre funcionarios de carrera del Estado, de las Comunidades Autónomas o de las Entidades Locales, pertenecientes a Cuerpos o Escalas clasificados como Subgrupo A1.

Los Directores Insulares dependen jerárquicamente del Delegado del Gobierno en la Comunidad Autónoma o del Subdelegado del Gobierno en la provincia, cuando este cargo exista, y ejercen, en su ámbito territorial, las competencias atribuidas por esta Ley a los Subdelegados del Gobierno en las provincias.

Artículo 71. *Los servicios territoriales.*

1. Los servicios territoriales de la Administración General del Estado en la Comunidad Autónoma se organizarán atendiendo al mejor cumplimiento de sus fines, en servicios integrados y no integrados en las Delegaciones del Gobierno.

2. La organización de los servicios territoriales no integrados en las Delegaciones del Gobierno se establecerá mediante Real Decreto a propuesta conjunta del titular del Ministerio del que dependan y del titular del Ministerio que tenga atribuida la competencia para la racionalización, análisis y evaluación de las estructuras organizativas de la Administración General del Estado y sus organismos públicos, cuando contemple unidades con nivel de Subdirección General o equivalentes, o por Orden conjunta cuando afecte a órganos inferiores.

3. Los servicios territoriales no integrados dependerán del órgano central competente sobre el sector de actividad en el que aquéllos operen, el cual les fijará los objetivos concretos de actuación y controlará su ejecución, así como el funcionamiento de los servicios.

4. Los servicios territoriales integrados dependerán del Delegado del Gobierno, o en su caso Subdelegado del Gobierno, a través de la Secretaría General, y actuarán de acuerdo con las instrucciones técnicas y criterios operativos establecidos por el Ministerio competente por razón de la materia.

Sección 2.ª Los Delegados del Gobierno en las Comunidades Autónomas

Artículo 72. *Los Delegados del Gobierno en las Comunidades Autónomas.*

1. Los Delegados del Gobierno representan al Gobierno de la Nación en el territorio de la respectiva Comunidad Autónoma, sin perjuicio de la representación ordinaria del Estado en las mismas a través de sus respectivos Presidentes.

2. Los Delegados del Gobierno dirigirán y supervisarán la Administración General del Estado en el territorio de las respectivas Comunidades Autónomas y la coordinarán, internamente y cuando proceda, con la administración propia de cada una de ellas y con la de las Entidades Locales radicadas en la Comunidad.

3. Los Delegados del Gobierno son órganos directivos con rango de Subsecretario que dependen orgánicamente del Presidente del Gobierno y funcionalmente del Ministerio competente por razón de la materia.

4. Los Delegados del Gobierno serán nombrados y separados por Real Decreto del Consejo de Ministros, a propuesta del Presidente del Gobierno. Su nombramiento atenderá a criterios de competencia profesional y experiencia. En todo caso, deberá reunir los requisitos de idoneidad establecidos en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

5. En caso de ausencia, vacante o enfermedad del titular de la Delegación del Gobierno, será suplido por el Subdelegado del Gobierno que el Delegado designe y, en su defecto, al de la provincia en que tenga su sede. En las Comunidades Autónomas uniprovinciales en las que no exista Subdelegado la suplencia corresponderá al Secretario General.

Artículo 73. *Competencias de los Delegados del Gobierno en las Comunidades Autónomas.*

1. Los Delegados del Gobierno en las Comunidades Autónomas son los titulares de las correspondientes Delegaciones del Gobierno y tienen, en los términos establecidos en este Capítulo, las siguientes competencias:

a) Dirección y coordinación de la Administración General del Estado y sus Organismos públicos:

1.º Impulsar, coordinar y supervisar con carácter general su actividad en el territorio de la Comunidad Autónoma, y, cuando se trate de servicios integrados, dirigirla, directamente o a través de los subdelegados del gobierno, de acuerdo con los objetivos y, en su caso, instrucciones de los órganos superiores de los respectivos ministerios.

2.º Nombrar a los Subdelegados del Gobierno en las provincias de su ámbito de actuación y, en su caso, a los Directores Insulares, y como superior jerárquico, dirigir y coordinar su actividad.

3.º Informar, con carácter preceptivo, las propuestas de nombramiento de los titulares de órganos territoriales de la Administración General del Estado y los Organismos públicos estatales de ámbito autonómico y provincial en la Delegación del Gobierno.

b) Información de la acción del Gobierno e información a los ciudadanos:

1.º Coordinar la información sobre los programas y actividades del Gobierno y la Administración General del Estado y sus Organismos públicos en la Comunidad Autónoma.

2.º Promover la colaboración con las restantes Administraciones Públicas en materia de información al ciudadano.

3.º Recibir información de los distintos Ministerios de los planes y programas que hayan de ejecutar sus respectivos servicios territoriales y Organismos públicos en su ámbito territorial.

4.º Elevar al Gobierno, con carácter anual, a través del titular del Ministerio de Hacienda y Administraciones Públicas, un informe sobre el funcionamiento de los servicios públicos estatales en el ámbito autonómico.

c) Coordinación y colaboración con otras Administraciones Públicas:

1.º Comunicar y recibir cuanta información precisen el Gobierno y el órgano de Gobierno de la Comunidad Autónoma. Realizará también estas funciones con las Entidades Locales en su ámbito territorial, a través de sus respectivos Presidentes.

2.º Mantener las necesarias relaciones de coordinación y cooperación de la Administración General del Estado y sus Organismos públicos con la de la Comunidad Autónoma y con las correspondientes Entidades Locales. A tal fin, promoverá la celebración de convenios con la Comunidad Autónoma y con las Entidades Locales, en particular, en relación a los programas de financiación estatal, participando en el seguimiento de la ejecución y cumplimiento de los mismos.

3.º Participar en las Comisiones mixtas de transferencias y en las Comisiones bilaterales de cooperación, así como en otros órganos de cooperación de naturaleza similar cuando se determine.

d) Control de legalidad:

1.º Resolver los recursos en vía administrativa interpuestos contra las resoluciones y actos dictados por los órganos de la Delegación, previo informe, en todo caso, del Ministerio competente por razón de la materia.

Las impugnaciones de resoluciones y actos del Delegado del Gobierno susceptibles de recurso administrativo y que no pongan fin a la vía administrativa, serán resueltas por los órganos correspondientes del Ministerio competente por razón de la materia.

Las reclamaciones por responsabilidad patrimonial de las Administraciones Públicas se tramitarán por el Ministerio competente por razón de la materia y se resolverán por el titular de dicho Departamento.

2.º Suspender la ejecución de los actos impugnados dictados por los órganos de la Delegación del Gobierno, cuando le corresponda resolver el recurso, de acuerdo con el artículo 117.2 de la Ley del Procedimiento Administrativo Común de las Administraciones Públicas, y proponer la suspensión en los restantes casos, así como respecto de los actos impugnados dictados por los servicios no integrados en la Delegación del Gobierno.

3.º Velar por el cumplimiento de las competencias atribuidas constitucionalmente al Estado y por la correcta aplicación de su normativa, promoviendo o interponiendo, según corresponda, conflictos de jurisdicción, conflictos de atribuciones, recursos y demás acciones legalmente procedentes.

e) Políticas públicas:

1.º Formular a los Ministerios competentes, en cada caso, las propuestas que estime convenientes sobre los objetivos contenidos en los planes y programas que hayan de ejecutar los servicios territoriales y los de los Organismos públicos, e informar, regular y periódicamente, a los Ministerios competentes sobre la gestión de sus servicios territoriales.

2.º Proponer ante el Ministro de Hacienda y Administraciones Públicas las medidas precisas para evitar la duplicidad de estructuras administrativas, tanto en la propia Administración General del Estado como con otras Administraciones Públicas, conforme a los principios de eficacia y eficiencia.

3.º Proponer al Ministerio de Hacienda y Administraciones Públicas medidas para incluir en los planes de recursos humanos de la Administración General del Estado.

4.º Informar las medidas de optimización de recursos humanos y materiales en su ámbito territorial, especialmente las que afecten a más de un Departamento. En particular, corresponde a los Delegados del Gobierno, en los términos establecidos en la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, la coordinación de la utilización de los edificios de uso administrativo por la organización territorial de la Administración General del Estado y de los organismos públicos de ella dependientes en su ámbito territorial, de acuerdo con las directrices establecidas por el Ministerio de Hacienda y Administraciones Públicas y la Dirección General del Patrimonio del Estado.

2. Asimismo, los Delegados del Gobierno ejercerán la potestad sancionadora, expropiatoria y cualesquiera otras que les confieran las normas o que les sean desconcentradas o delegadas.

3. Corresponde a los Delegados del Gobierno proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana, a través de los Subdelegados del Gobierno y de las Fuerzas y Cuerpos de seguridad del Estado, cuya jefatura corresponderá al Delegado del Gobierno, quien ejercerá las competencias del Estado en esta materia bajo la dependencia funcional del Ministerio del Interior.

4. En relación con los servicios territoriales, los Delegados del Gobierno, para el ejercicio de las competencias recogidas en este artículo, podrán recabar de los titulares de dichos servicios toda la información relativa a su actividad, estructuras organizativas, recursos humanos, inventarios de bienes muebles e inmuebles o a cualquier otra materia o asunto que consideren oportuno al objeto de garantizar una gestión coordinada y eficaz de los servicios estatales en el territorio.

Sección 3.ª Los Subdelegados del Gobierno en las provincias

Artículo 74. *Los Subdelegados del Gobierno en las provincias.*

En cada provincia y bajo la inmediata dependencia del Delegado del Gobierno en la respectiva Comunidad Autónoma, existirá un Subdelegado del Gobierno, con nivel de Subdirector General, que será nombrado por aquél mediante el procedimiento de libre designación entre funcionarios de carrera del Estado, de las Comunidades Autónomas o de las Entidades Locales, pertenecientes a Cuerpos o Escalas clasificados como Subgrupo A1.

En las Comunidades Autónomas uniprovinciales en las que no exista Subdelegado, el Delegado del Gobierno asumirá las competencias que esta Ley atribuye a los Subdelegados del Gobierno en las provincias.

Artículo 75. *Competencias de los Subdelegados del Gobierno en las provincias.*

A los Subdelegados del Gobierno les corresponde:

a) Desempeñar las funciones de comunicación, colaboración y cooperación con la respectiva Comunidad Autónoma y con las Entidades Locales y, en particular, informar sobre la incidencia en el territorio de los programas de financiación estatal. En concreto les corresponde:

1.º Mantener las necesarias relaciones de cooperación y coordinación de la Administración General del Estado y sus Organismos públicos con la de la Comunidad Autónoma y con las correspondientes Entidades locales en el ámbito de la provincia.

2.º Comunicar y recibir cuanta información precisen el Gobierno y el órgano de Gobierno de la Comunidad Autónoma. Realizará también estas funciones con las Entidades locales en su ámbito territorial, a través de sus respectivos Presidentes.

b) Proteger el libre ejercicio de los derechos y libertades, garantizando la seguridad ciudadana, todo ello dentro de las competencias estatales en la materia. A estos efectos, dirigirá las Fuerzas y Cuerpos de Seguridad del Estado en la provincia.

c) Dirigir y coordinar la protección civil en el ámbito de la provincia.

d) Dirigir, en su caso, los servicios integrados de la Administración General del Estado, de acuerdo con las instrucciones del Delegado del Gobierno y de los Ministerios correspondientes; e impulsar, supervisar e inspeccionar los servicios no integrados.

e) Coordinar la utilización de los medios materiales y, en particular, de los edificios administrativos en el ámbito territorial de su competencia.

f) Ejercer la potestad sancionadora y cualquier otra que les confiera las normas o que les sea desconcentrada o delegada.

Sección 4.ª La estructura de las delegaciones del gobierno

Artículo 76. *Estructura de las Delegaciones y Subdelegaciones del Gobierno.*

1. La estructura de las Delegaciones y Subdelegaciones del Gobierno se fijará por Real Decreto del Consejo de Ministros a propuesta del Ministerio de Hacienda y Administraciones Públicas, en razón de la dependencia orgánica de las Delegaciones del Gobierno, y contarán, en todo caso, con una Secretaría General, dependiente de los Delegados o, en su caso, de los Subdelegados del Gobierno, como órgano de gestión de los servicios comunes, y de la que dependerán los distintos servicios integrados en la misma, así como aquellos otros servicios y unidades que se determine en la relación de puestos de trabajo.

2. La integración de nuevos servicios territoriales o la desintegración de servicios territoriales ya integrados en las Delegaciones del Gobierno, se llevará a cabo mediante Real Decreto de Consejo de Ministros, a propuesta del Ministerio de Hacienda y Administraciones Públicas, en razón de la dependencia orgánica de las Delegaciones del Gobierno, y del Ministerio competente del área de actividad.

Artículo 77. *Asistencia jurídica y control económico financiero de las Delegaciones y Subdelegaciones del Gobierno.*

La asistencia jurídica y las funciones de intervención y control económico financiero en relación con las Delegaciones y Subdelegaciones del Gobierno se ejercerán por la Abogacía del Estado y la Intervención General de la Administración del Estado respectivamente, de acuerdo con su normativa específica.

Sección 5.ª Órganos colegiados

Artículo 78. *La Comisión interministerial de coordinación de la Administración periférica del Estado.*

1. La Comisión interministerial de coordinación de la Administración periférica del Estado es un órgano colegiado, adscrito al Ministerio de Hacienda y Administraciones Públicas.
2. La Comisión interministerial de coordinación de la Administración periférica del Estado se encargará de coordinar la actuación de la Administración periférica del Estado con los distintos Departamentos ministeriales.
3. Mediante Real Decreto se regularán sus atribuciones, composición y funcionamiento.

Artículo 79. *Los órganos colegiados de asistencia al Delegado y al Subdelegado del Gobierno.*

1. En cada una de las Comunidades Autónomas pluriprovinciales existirá una Comisión territorial de asistencia al Delegado del Gobierno, con las siguientes características:

a) Estará presidida por el Delegado del Gobierno en la Comunidad Autónoma e integrada por los Subdelegados del Gobierno en las provincias comprendidas en el territorio de ésta.
b) A sus sesiones deberán asistir los titulares de los órganos y servicios territoriales, tanto integrados como no integrados, que el Delegado del Gobierno considere oportuno.
c) Esta Comisión desarrollará, en todo caso, las siguientes funciones:

1.º Coordinar las actuaciones que hayan de ejecutarse de forma homogénea en el ámbito de la Comunidad Autónoma, para asegurar el cumplimiento de los objetivos generales fijados por el Gobierno a los servicios territoriales.
2.º Homogeneizar el desarrollo de las políticas públicas en su ámbito territorial, a través del establecimiento de criterios comunes de actuación que habrán de ser compatibles con las instrucciones y objetivos de los respectivos departamentos ministeriales.
3.º Asesorar al Delegado del Gobierno en la Comunidad Autónoma en la elaboración de las propuestas de simplificación administrativa y racionalización en la utilización de los recursos.
4.º Cualesquiera otras que a juicio del Delegado del Gobierno en la Comunidad Autónoma resulten adecuadas para que la Comisión territorial cumpla la finalidad de apoyo y asesoramiento en el ejercicio de las competencias que esta Ley le asigna.

2. En las Comunidades Autónomas uniprovinciales existirá una Comisión de asistencia al Delegado del Gobierno, presidida por él mismo e integrada por el Secretario General y los titulares de los órganos y servicios territoriales, tanto integrados como no integrados, que el Delegado del Gobierno considere oportuno, con las funciones señaladas en el apartado anterior.
3. En cada Subdelegación del Gobierno existirá una Comisión de asistencia al Subdelegado del Gobierno presidida por él mismo e integrada por el Secretario General y los titulares de los órganos y servicios territoriales, tanto integrados como no integrados, que el Subdelegado del Gobierno considere oportuno, con las funciones señaladas en el apartado primero, referidas al ámbito provincial.

CAPÍTULO IV

De la Administración General del Estado en el exterior

Artículo 80. *El Servicio Exterior del Estado.*

El Servicio Exterior del Estado se rige en todo lo concerniente a su composición, organización, funciones, integración y personal por lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado y en su normativa de desarrollo y, supletoriamente, por lo dispuesto en esta Ley.

TÍTULO II

Organización y funcionamiento del sector público institucional

CAPÍTULO I

Del sector público institucional

Artículo 81. *Principios generales de actuación.*

1. Las entidades que integran el sector público institucional están sometidas en su actuación a los principios de legalidad, eficiencia, estabilidad presupuestaria y sostenibilidad financiera así como al principio de transparencia en su gestión. En particular se sujetarán en materia de personal, incluido el laboral, a las limitaciones previstas en la normativa presupuestaria y en las previsiones anuales de los presupuestos generales.

2. Todas las Administraciones Públicas deberán establecer un sistema de supervisión continua de sus entidades dependientes, con el objeto de comprobar la subsistencia de los motivos que justificaron su creación y su sostenibilidad financiera, y que deberá incluir la formulación expresa de propuestas de mantenimiento, transformación o extinción.

3. Los organismos y entidades vinculados o dependientes de la Administración autonómica y local se regirán por las disposiciones básicas de esta ley que les resulten de aplicación, y en particular, por lo dispuesto en los Capítulos I y VI y en los artículos 129 y 134, así como por la normativa propia de la Administración a la que se adscriban.

Artículo 82. *El Inventario de Entidades del Sector Público Estatal, Autonómico y Local.*

1. El Inventario de Entidades del Sector Público Estatal, Autonómico y Local, se configura como un registro público administrativo que garantiza la información pública y la ordenación de todas las entidades integrantes del sector público institucional cualquiera que sea su naturaleza jurídica.

La integración y gestión de dicho Inventario y su publicación dependerá de la Intervención General de la Administración del Estado.

2. El Inventario de Entidades del Sector Público contendrá, al menos, información actualizada sobre la naturaleza jurídica, finalidad, fuentes de financiación, estructura de dominio, en su caso, la condición de medio propio, regímenes de contabilidad, presupuestario y de control así como la clasificación en términos de contabilidad nacional, de cada una de las entidades integrantes del sector público institucional.

3. Al menos, la creación, transformación, fusión o extinción de cualquier entidad integrante del sector público institucional, cualquiera que sea su naturaleza jurídica, será inscrita en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local.

Artículo 83. *Inscripción en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local.*

1. El titular del máximo órgano de dirección de la entidad notificará, a través de la intervención general de la Administración correspondiente, la información necesaria para la inscripción definitiva en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local, en los términos previstos reglamentariamente, de los actos relativos a su creación, transformación, fusión o extinción, en el plazo de treinta días hábiles a contar desde que

ocurra el acto inscribible. En la citada notificación se acompañará la documentación justificativa que determina tal circunstancia.

2. La inscripción definitiva de la creación de cualquier entidad integrante del sector público institucional en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local se realizará de conformidad con las siguientes reglas:

a) El titular del máximo órgano de dirección de la entidad, a través de la intervención general de la Administración correspondiente, notificará, electrónicamente a efectos de su inscripción, al Inventario de Entidades del Sector Público Estatal, Autonómico y Local, la norma o el acto jurídico de creación en el plazo de 30 días hábiles desde la entrada en vigor de la norma o del acto, según corresponda. A la notificación se acompañará la copia o enlace a la publicación electrónica del Boletín Oficial en el que se publicó la norma, o copia del acto jurídico de creación, así como el resto de documentación justificativa que proceda, como los Estatutos o el plan de actuación.

b) La inscripción en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local se practicará dentro del plazo de 15 días hábiles siguientes a la recepción de la solicitud de inscripción.

c) Para la asignación del Número de Identificación Fiscal definitivo y de la letra identificativa que corresponda a la entidad, de acuerdo con su naturaleza jurídica, por parte de la Administración Tributaria será necesaria la aportación de la certificación de la inscripción de la entidad en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local.

CAPÍTULO II

Organización y funcionamiento del sector público institucional estatal

Artículo 84. *Composición y clasificación del sector público institucional estatal.*

1. Integran el sector público institucional estatal las siguientes entidades:

a) Los organismos públicos vinculados o dependientes de la Administración General del Estado, los cuales se clasifican en:

1. Organismos autónomos.
2. Entidades públicas empresariales.
3. Agencias estatales.

b) Las autoridades administrativas independientes.
c) Las sociedades mercantiles estatales.
d) Los consorcios.
e) Las fundaciones del sector público.
f) Los fondos sin personalidad jurídica.
g) Las universidades públicas no transferidas.

2. La Administración General del Estado o entidad integrante del sector público institucional estatal no podrá, por sí misma ni en colaboración con otras entidades públicas o privadas, crear, ni ejercer el control efectivo, directa ni indirectamente, sobre ningún otro tipo de entidad distinta de las enumeradas en este artículo, con independencia de su naturaleza y régimen jurídico.

Lo dispuesto en este apartado no será de aplicación a la participación del Estado en organismos internacionales o entidades de ámbito supranacional, ni a la participación en los organismos de normalización y acreditación nacionales o en sociedades creadas al amparo de la Ley 27/1984, de 26 de julio, sobre reconversión y reindustrialización.

3. Las universidades públicas no transferidas se regirán por lo dispuesto en la Ley 47/2003, de 26 de noviembre, que les sea de aplicación y por lo dispuesto en esta ley en lo que no esté previsto en su normativa específica.

Artículo 85. *Control de eficacia y supervisión continua.*

1. Las entidades integrantes del sector público institucional estatal estarán sometidas al control de eficacia y supervisión continua, sin perjuicio de lo establecido en el artículo 110.

Para ello, todas las entidades integrantes del sector público institucional estatal contarán, en el momento de su creación, con un plan de actuación, que contendrá las líneas estratégicas en torno a las cuales se desenvolverá la actividad de la entidad, que se revisarán cada tres años, y que se completará con planes anuales que desarrollarán el de creación para el ejercicio siguiente.

2. El control de eficacia será ejercido por el Departamento al que estén adscritos, a través de las inspecciones de servicios, y tendrá por objeto evaluar el cumplimiento de los objetivos propios de la actividad específica de la entidad y la adecuada utilización de los recursos, de acuerdo con lo establecido en su plan de actuación y sus actualizaciones anuales, sin perjuicio del control que de acuerdo con la Ley 47/2003, de 26 de noviembre, se ejerza por la Intervención General de la Administración del Estado.

3. Todas las entidades integrantes del sector público institucional estatal están sujetas desde su creación hasta su extinción a la supervisión continua del Ministerio de Hacienda y Administraciones Públicas, a través de la Intervención General de la Administración del Estado, que vigilará la concurrencia de los requisitos previstos en esta Ley. En particular verificará, al menos, lo siguiente:

a) La subsistencia de las circunstancias que justificaron su creación.

b) Su sostenibilidad financiera.

c) La concurrencia de la causa de disolución prevista en esta ley referida al incumplimiento de los fines que justificaron su creación o que su subsistencia no resulte el medio más idóneo para lograrlos.

Las actuaciones de planificación, ejecución y evaluación correspondientes a la supervisión continua se determinarán reglamentariamente.

4. Las actuaciones de control de eficacia y supervisión continua tomarán en consideración:

a) La información económico financiera disponible.

b) El suministro de información por parte de los organismos públicos y entidades sometidas al Sistema de control de eficacia y supervisión continúa.

c) Las propuestas de las inspecciones de los servicios de los departamentos ministeriales.

Los resultados de la evaluación efectuada tanto por el Ministerio de adscripción como por el Ministerio de Hacienda y Administraciones Públicas se plasmarán en un informe sujeto a procedimiento contradictorio que, según las conclusiones que se hayan obtenido, podrá contener recomendaciones de mejora o una propuesta de transformación o supresión del organismo público o entidad.

Artículo 86. *Medio propio y servicio técnico.*

1. Las entidades integrantes del sector público institucional podrán ser consideradas medios propios y servicios técnicos de los poderes adjudicadores y del resto de entes y sociedades que no tengan la consideración de poder adjudicador cuando cumplan las condiciones y requisitos establecidos en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

2. Tendrán la consideración de medio propio y servicio técnico cuando se acredite que, además de disponer de medios suficientes e idóneos para realizar prestaciones en el sector de actividad que se corresponda con su objeto social, de acuerdo con su norma o acuerdo de creación, se dé alguna de las circunstancias siguientes:

a) Sea una opción más eficiente que la contratación pública y resulta sostenible y eficaz, aplicando criterios de rentabilidad económica.

b) Resulte necesario por razones de seguridad pública o de urgencia en la necesidad de disponer de los bienes o servicios suministrados por el medio propio o servicio técnico.

Formará parte del control de eficacia de los medios propios y servicios técnicos la comprobación de la concurrencia de los mencionados requisitos.

En la denominación de las entidades integrantes del sector público institucional que tengan la condición de medio propio deberá figurar necesariamente la indicación ‘‘Medio Propio’’ o su abreviatura “M.P.”.

3. En el supuesto de creación de un nuevo medio propio y servicio técnico deberá acompañarse la propuesta de declaración de una memoria justificativa que acredite lo dispuesto en el apartado anterior y que, en este supuesto de nueva creación, deberá ser informada por la Intervención General de la Administración del Estado.

Artículo 87. *Transformaciones de las entidades integrantes del sector público institucional estatal.*

1. Cualquier organismo autónomo, entidad pública empresarial, agencias estatales, sociedad mercantil estatal o fundación del sector público institucional estatal podrá transformarse y adoptar la naturaleza jurídica de cualquiera de las entidades citadas.

2. La transformación tendrá lugar, conservando su personalidad jurídica, por cesión e integración global, en unidad de acto, de todo el activo y el pasivo de la entidad transformada con sucesión universal de derechos y obligaciones.

La transformación no alterará las condiciones financieras de las obligaciones asumidas ni podrá ser entendida como causa de resolución de las relaciones jurídicas.

3. La transformación se llevará a cabo mediante Real Decreto, aunque suponga modificación de la Ley de creación, salvo en el caso de la transformación en agencias estatales que deberá efectuarse por ley.

4. Cuando un organismo autónomo, entidad pública empresarial o Agencias Estatales se transforme en una entidad pública empresarial, Agencias Estatales, sociedad mercantil estatal o en una fundación del sector público, el Real Decreto o la Ley mediante el que se lleve a cabo la transformación deberá ir acompañado de la siguiente documentación:

a) Una memoria que incluya:

1.º Una justificación de la transformación por no poder asumir sus funciones manteniendo su naturaleza jurídica originaria.

2.º Un análisis de eficiencia que incluirá una previsión del ahorro que generará la transformación y la acreditación de inexistencia de duplicidades con las funciones que ya desarrolle otro órgano, organismo público o entidad preexistente.

3.º Un análisis de la situación en la que quedará el personal, indicando si, en su caso, parte del mismo se integrará, bien en la Administración General del Estado o bien en la entidad pública empresarial, sociedad mercantil estatal o fundación que resulte de la transformación.

b) Un informe preceptivo de la Intervención General de la Administración del Estado en el que se valorará el cumplimiento de lo previsto en este artículo.

5. La aprobación del Real Decreto de transformación conllevará:

a) La adaptación de la organización de los medios personales, materiales y económicos que resulte necesaria por el cambio de naturaleza jurídica.

b) La posibilidad de integrar el personal en la entidad transformada o en la Administración General del Estado. En su caso, esta integración se llevará a cabo de acuerdo con los procedimientos de movilidad establecidos en la legislación de función pública o en la legislación laboral que resulte aplicable.

Los distintos tipos de personal de la entidad transformada tendrán los mismos derechos y obligaciones que les correspondan de acuerdo con la normativa que les sea de aplicación.

La adaptación, en su caso, de personal que conlleve la transformación no supondrá, por sí misma, la atribución de la condición de funcionario público al personal laboral que prestase servicios en la entidad transformada.

La integración de quienes hasta ese momento vinieran ejerciendo funciones reservadas a funcionarios públicos sin serlo podrá realizarse con la condición de “a extinguir”,

debiéndose valorar previamente las características de los puestos afectados y las necesidades de la entidad donde se integren.

De la ejecución de las medidas de transformación no podrá derivarse incremento alguno de la masa salarial preexistente en la entidad transformada.

CAPÍTULO III

De los organismos públicos estatales

Sección 1.ª Disposiciones generales

Artículo 88. *Definición y actividades propias.*

Son organismos públicos dependientes o vinculados a la Administración General del Estado, bien directamente o bien a través de otro organismo público, los creados para la realización de actividades administrativas, sean de fomento, prestación o de gestión de servicios públicos o de producción de bienes de interés público susceptibles de contraprestación; actividades de contenido económico reservadas a las Administraciones Públicas; así como la supervisión o regulación de sectores económicos, y cuyas características justifiquen su organización en régimen de descentralización funcional o de independencia.

Artículo 89. *Personalidad jurídica y potestades.*

1. Los organismos públicos tiene personalidad jurídica pública diferenciada, patrimonio y tesorería propios, así como autonomía de gestión, en los términos previstos en esta Ley.

2. Dentro de su esfera de competencia, les corresponden las potestades administrativas precisas para el cumplimiento de sus fines, en los términos que prevean sus estatutos, salvo la potestad expropiatoria.

Los estatutos podrán atribuir a los organismos públicos la potestad de ordenar aspectos secundarios del funcionamiento para cumplir con los fines y el servicio encomendado, en el marco y con el alcance establecido por las disposiciones que fijen el régimen jurídico básico de dicho servicio.

Los actos y resoluciones dictados por los organismos públicos en el ejercicio de potestades administrativas son susceptibles de los recursos administrativos previstos en la Ley del Procedimiento Administrativo Común de las Administraciones Públicas.

Artículo 90. *Estructura organizativa en el sector público estatal.*

1. Los organismos públicos se estructuran en los órganos de gobierno, y ejecutivos que se determinen en su respectivo Estatuto.

Los máximos órganos de gobierno son el Presidente y el Consejo Rector. El estatuto puede, no obstante, prever otros órganos de gobierno con atribuciones distintas.

La dirección del organismo público debe establecer un modelo de control orientado a conseguir una seguridad razonable en el cumplimiento de sus objetivos.

2. Corresponde al Ministro de Hacienda y Administraciones Públicas la clasificación de las entidades, conforme a su naturaleza y a los criterios previstos en Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos en el sector público empresarial y otras entidades. A estos efectos, las entidades serán clasificadas en tres grupos. Esta clasificación determinará el nivel en que la entidad se sitúa a efectos de:

a) Número máximo de miembros de los órganos de gobierno.

b) Estructura organizativa, con fijación del número mínimo y máximo de directivos, así como la cuantía máxima de la retribución total, con determinación del porcentaje máximo del complemento de puesto y variable.

Artículo 91. *Creación de organismos públicos estatales.*

1. La creación de los organismos públicos se efectuará por Ley.

2. La Ley de creación establecerá:

a) El tipo de organismo público que crea, con indicación de sus fines generales, así como el Departamento de dependencia o vinculación.

b) En su caso, los recursos económicos, así como las peculiaridades de su régimen de personal, de contratación, patrimonial, fiscal y cualesquiera otras que, por su naturaleza, exijan norma con rango de Ley.

3. El anteproyecto de ley de creación del organismo público que se eleve al Consejo de Ministros deberá ser acompañado de una propuesta de estatutos y de un plan inicial de actuación, junto con el informe preceptivo favorable del Ministerio de Hacienda y Administraciones Públicas que valorará el cumplimiento de lo previsto en este artículo.

Artículo 92. *Contenido y efectos del plan de actuación.*

1. El plan inicial de actuación contendrá, al menos:

a) Las razones que justifican la creación de un nuevo organismo público, por no poder asumir esas funciones otro ya existente, así como la constatación de que la creación no supone duplicidad con la actividad que desarrolle cualquier otro órgano o entidad preexistente.

b) La forma jurídica propuesta y un análisis que justifique que la elegida resulta más eficiente frente a otras alternativas de organización que se hayan descartado.

c) La fundamentación de la estructura organizativa elegida, determinando los órganos directivos y la previsión sobre los recursos humanos necesarios para su funcionamiento.

d) El anteproyecto del presupuesto correspondiente al primer ejercicio junto con un estudio económico-financiero que acredite la suficiencia de la dotación económica prevista inicialmente para el comienzo de su actividad y la sostenibilidad futura del organismo, atendiendo a las fuentes futuras de financiación de los gastos y las inversiones, así como a la incidencia que tendrá sobre los presupuestos generales del Estado.

e) Los objetivos del organismo, justificando su suficiencia o idoneidad, los indicadores para medirlos, y la programación plurianual de carácter estratégico para alcanzarlos, especificando los medios económicos y personales que dedicará, concretando en este último caso la forma de provisión de los puestos de trabajo, su procedencia, coste, retribuciones e indemnizaciones, así como el ámbito temporal en que se prevé desarrollar la actividad del organismo. Asimismo, se incluirán las consecuencias asociadas al grado de cumplimiento de los objetivos establecidos y, en particular, su vinculación con la evaluación de la gestión del personal directivo en el caso de incumplimiento. A tal efecto, el reparto del complemento de productividad o concepto equivalente se realizará teniendo en cuenta el grado de cumplimiento de los objetivos establecidos en el plan de creación y en los anuales.

2. Los organismos públicos deberán acomodar su actuación a lo previsto en su plan inicial de actuación. Éste se actualizará anualmente mediante la elaboración del correspondiente plan que permita desarrollar para el ejercicio siguiente las previsiones del plan de creación. El plan anual de actuación deberá ser aprobado en el último trimestre del año natural por el departamento del que dependa o al que esté vinculado el organismo y deberá guardar coherencia con el Programa de actuación plurianual previsto en la normativa presupuestaria. El Plan de actuación incorporará, cada tres años, una revisión de la programación estratégica del organismo.

La falta de aprobación del plan anual de actuación dentro del plazo fijado por causa imputable al organismo, y hasta tanto se subsane la omisión, llevará aparejada la paralización de las transferencias que deban realizarse a favor del organismo con cargo a los Presupuestos Generales del Estado, salvo que el Consejo de Ministros adopte otra decisión.

3. El plan de actuación y los anuales, así como sus modificaciones, se hará público en la página web del organismo público al que corresponda.

Artículo 93. *Contenido de los estatutos.*

1. Los estatutos regularán, al menos, los siguientes extremos:

a) Las funciones y competencias del organismo, con indicación de las potestades administrativas que pueda ostentar.

b) La determinación de su estructura organizativa, con expresión de la composición, funciones, competencias y rango administrativo que corresponda a cada órgano. Asimismo se especificarán aquellos de sus actos y resoluciones que agoten la vía administrativa.

c) El patrimonio que se les asigne y los recursos económicos que hayan de financiarlos.

d) El régimen relativo a recursos humanos, patrimonio, presupuesto y contratación.

e) La facultad de participación en sociedades mercantiles cuando ello sea imprescindible para la consecución de los fines asignados.

2. Los estatutos de los organismos públicos se aprobarán por Real Decreto del Consejo de Ministros a propuesta conjunta del Ministerio de Hacienda y Administraciones Públicas y del Ministerio al que el organismo esté vinculado o sea dependiente.

3. Los estatutos deberán ser aprobados y publicados con carácter previo a la entrada en funcionamiento efectivo del organismo público.

Artículo 94. *Fusión de organismos públicos estatales.*

1. Los organismos públicos estatales de la misma naturaleza jurídica podrán fusionarse bien mediante su extinción e integración en un nuevo organismo público, bien mediante su extinción por ser absorbido por otro organismo público ya existente.

2. La fusión se llevará a cabo mediante norma reglamentaria, aunque suponga modificación de la Ley de creación. Cuando la norma reglamentaria cree un nuevo organismo público resultante de la fusión deberá cumplir con lo previsto en el artículo 91.2 sobre requisitos de creación de organismos públicos.

3. A la norma reglamentaria de fusión se acompañará un plan de redimensionamiento para la adecuación de las estructuras organizativas, inmobiliarias, de personal y de recursos resultantes de la nueva situación y en el que debe quedar acreditado el ahorro que generará la fusión.

Si alguno de los organismos públicos estuviese en situación de desequilibrio financiero se podrá prever, como parte del plan de redimensionamiento, que las obligaciones, bienes y derechos patrimoniales que se consideren liquidables y derivados de la actividad que ocasionó el desequilibrio, se integren en un fondo, sin personalidad jurídica y con contabilidad separada, adscrito al nuevo organismo público o al absorbente, según corresponda.

La actividad o actividades que ocasionaron el desequilibrio dejarán de prestarse tras la fusión, salvo que se prevea su realización futura de forma sostenible tras la fusión.

El plan de redimensionamiento, previo informe preceptivo de la Intervención General de la Administración del Estado deberá ser aprobado por cada uno de los organismos públicos fusionados si se integran en uno nuevo o por el organismo público absorbente, según corresponda al tipo de fusión.

4. La aprobación de la norma de fusión conllevará:

a) La integración de las organizaciones de los organismos públicos fusionados, incluyendo los medios personales, materiales y económicos, en los términos previstos en el plan de redimensionamiento.

b) El personal de los organismos públicos extinguidos se podrá integrar bien en la Administración General del Estado o bien en el nuevo organismo público que resulte de la fusión o en el organismo público absorbente, según proceda, de acuerdo con lo previsto en la norma reglamentaria de fusión y de conformidad con los procedimientos de movilidad establecidos en la legislación de función pública o en la legislación laboral que resulte aplicable.

Los distintos tipos de personal de los organismos públicos fusionados tendrán los derechos y obligaciones que les correspondan de acuerdo con la normativa que les sea de aplicación.

La integración de quienes hasta ese momento vinieran ejerciendo funciones reservadas a funcionarios públicos sin serlo podrá realizarse con la condición de «a extinguir», debiéndose valorar previamente las características de los puestos afectados y las necesidades del organismos donde se integren.

Esta integración de personal no supondrá, en ningún caso, la atribución de la condición de funcionario público al personal laboral que prestase servicios en los organismos públicos fusionados.

De la ejecución de las medidas de fusión no podrá derivarse incremento alguno de la masa salarial en los organismos públicos afectados.

c) La cesión e integración global, en unidad de acto, de todo el activo y el pasivo de los organismos públicos extinguidos en el nuevo organismo público resultante de la fusión o en el organismo público absorbente, según proceda, que le sucederá universalmente en todos sus derechos y obligaciones.

La fusión no alterará las condiciones financieras de las obligaciones asumidas ni podrá ser entendida como causa de resolución de las relaciones jurídicas.

d) Si se hubiera previsto en el plan de redimensionamiento, las obligaciones, bienes y derechos patrimoniales que se consideren liquidables se integrarán en un fondo, sin personalidad jurídica y con contabilidad separada, adscrito al nuevo organismo público resultante de la fusión o al organismo público absorbente, según proceda, que designará un liquidador al que le corresponderá la liquidación de este fondo. Esta liquidación se efectuará de conformidad con lo previsto en el artículo 97.

La liquidación deberá llevarse a cabo durante los dos años siguientes a la aprobación de la norma reglamentaria de fusión, salvo que el Consejo de Ministros acuerde su prórroga, sin perjuicio de los posibles derechos que puedan corresponder a los acreedores. La aprobación de las normas a las que tendrá que ajustarse la contabilidad del fondo corresponderá al Ministro de Hacienda y Administraciones Públicas a propuesta de la Intervención General de la Administración del Estado.

Artículo 95. *Gestión compartida de servicios comunes.*

1. La norma de creación de los organismos públicos del sector público estatal incluirá la gestión compartida de algunos o todos los servicios comunes, salvo que la decisión de no compartirlos se justifique, en la memoria que acompañe a la norma de creación, en términos de eficiencia, conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, en razones de seguridad nacional o cuando la organización y gestión compartida afecte a servicios que deban prestarse de forma autónoma en atención a la independencia del organismo.

La organización y gestión de algunos o todos los servicios comunes se coordinará por el Ministerio de adscripción, por el Ministerio de Hacienda y Administraciones Públicas o por un organismo público vinculado o dependiente del mismo.

2. Se consideran servicios comunes de los organismos públicos, al menos, los siguientes:

a) Gestión de bienes inmuebles.
b) Sistemas de información y comunicación.
c) Asistencia jurídica.
d) Contabilidad y gestión financiera.
e) Publicaciones.
f) Contratación pública.

Artículo 96. *Disolución de organismos públicos estatales.*

1. Los Organismos públicos estatales deberán disolverse:

a) Por el transcurso del tiempo de existencia señalado en la ley de creación.

b) Porque la totalidad de sus fines y objetivos sean asumidos por los servicios de la Administración General del Estado.

c) Porque sus fines hayan sido totalmente cumplidos, de forma que no se justifique la pervivencia del organismo público, y así se haya puesto de manifiesto en el control de eficacia.

d) Cuando del seguimiento del plan de actuación resulte el incumplimiento de los fines que justificaron la creación del organismo o que su subsistencia no es el medio más idóneo para lograrlos y así se concluya en el control de eficacia o de supervisión continua.

e) Por cualquier otra causa establecida en los estatutos.

f) Cuando así lo acuerde el Consejo de Ministros siguiendo el procedimiento determinado al efecto en el acto jurídico que acuerde la disolución.

2. Cuando un organismo público incurra en alguna de las causas de disolución previstas en las letras a), b), c), d) o e) del apartado anterior, el titular del máximo órgano de dirección del organismo lo comunicará al titular del departamento de adscripción en el plazo de dos meses desde que concurra la causa de disolución. Transcurrido dicho plazo sin que se haya producido la comunicación y concurriendo la causa de disolución, el organismo público quedará automáticamente disuelto y no podrá realizar ningún acto jurídico, salvo los estrictamente necesarios para garantizar la eficacia de su liquidación y extinción.

En el plazo de dos meses desde la recepción de la comunicación a la que se refiere el párrafo anterior, el Consejo de Ministros adoptará el correspondiente acuerdo de disolución, en el que designará al órgano administrativo o entidad del sector público institucional estatal que asumirá las funciones de liquidador, y se comunicará al Inventario de Entidades del Sector Público Estatal, Autonómico y Local para su publicación. Transcurrido dicho plazo sin que el acuerdo de disolución haya sido publicado, el organismo público quedará automáticamente disuelto y no podrá realizar ningún acto jurídico, salvo los estrictamente necesarios para garantizar la eficacia de su liquidación y extinción.

Artículo 97. *Liquidación y extinción de organismos públicos estatales.*

1. Publicado el acuerdo de disolución al que se refiere el artículo anterior, o transcurridos los plazos en él establecidos sin que éste haya sido publicado, se entenderá automáticamente iniciada la liquidación.

2. La liquidación tendrá lugar por la cesión e integración global, en unidad de acto, de todo el activo y el pasivo del organismo público en la Administración General del Estado que le sucederá universalmente en todos sus derechos y obligaciones. El órgano o entidad designada como liquidador determinará, en cada caso, el órgano o entidad concreta, de la Administración General del Estado, donde se integrarán los elementos que forman parte del activo y del pasivo del organismo público liquidado.

La responsabilidad que le corresponda al empleado público como miembro de la entidad u órgano liquidador será directamente asumida por la entidad o la Administración General del Estado que lo designó. La Administración General del Estado podrá exigir de oficio al empleado público que designó a esos efectos la responsabilidad en que hubiera incurrido por los daños y perjuicios causados en sus bienes o derechos cuando hubiera concurrido dolo, culpa o negligencia graves, conforme a lo previsto en las Leyes administrativas en materia de responsabilidad patrimonial.

3. La Administración General del Estado quedará subrogada automáticamente en todas las relaciones jurídicas que tuviera el organismo público con sus acreedores, tanto de carácter principal como accesorias, a la fecha de adopción del acuerdo de disolución o, en su defecto, a la fecha en que concurriera la causa de disolución, incluyendo los activos y pasivos sobrevenidos. Esta subrogación no alterará las condiciones financieras de las obligaciones asumidas ni podrá ser entendida como causa de resolución de las relaciones jurídicas.

4. Formalizada la liquidación del organismo público se producirá su extinción automática.

Sección 2.ª Organismos autónomos estatales

Artículo 98. *Definición.*

1. Los organismos autónomos son entidades de derecho público, con personalidad jurídica propia, tesorería y patrimonio propios y autonomía en su gestión, que desarrollan actividades propias de la Administración Pública, tanto actividades de fomento, prestacionales, de gestión de servicios públicos o de producción de bienes de interés público, susceptibles de contraprestación, en calidad de organizaciones instrumentales diferenciadas y dependientes de ésta.

2. Los organismos autónomos dependen de la Administración General del Estado a la que corresponde su dirección estratégica, la evaluación de los resultados de su actividad y el control de eficacia.

3. Con independencia de cuál sea su denominación, cuando un organismo público tenga la naturaleza jurídica de organismo autónomo deberá figurar en su denominación la indicación «organismo autónomo» o su abreviatura «O.A.».

Artículo 99. *Régimen jurídico.*

Los organismos autónomos se regirán por lo dispuesto en esta Ley, en su ley de creación, sus estatutos, la Ley de Procedimiento Administrativo Común de las Administraciones Públicas, el Real Decreto Legislativo 3/2011, de 14 de noviembre, la Ley 33/2003, de 3 de noviembre, y el resto de las normas de derecho administrativo general y especial que le sea de aplicación. En defecto de norma administrativa, se aplicará el derecho común.

Artículo 100. *Régimen jurídico del personal y de contratación.*

1. El personal al servicio de los organismos autónomos será funcionario o laboral, y se regirá por lo previsto en la Ley 7/2007, de 12 de abril, y demás normativa reguladora de los funcionarios públicos y por la normativa laboral.

El nombramiento de los titulares de los órganos de los organismos autónomos se regirá por las normas aplicables a la Administración General del Estado.

El titular del máximo órgano de dirección del organismo tendrá atribuidas, en materia de gestión de recursos humanos, las facultades que le asigne la legislación específica.

El organismo autónomo estará obligado a aplicar las instrucciones sobre recursos humanos dictadas por el Ministerio de Hacienda y Administraciones Públicas y a comunicarle a este departamento cuantos acuerdos o resoluciones adopte en aplicación del régimen específico de personal establecido en su Ley de creación o en sus estatutos.

2. La contratación de los organismos autónomos se ajustará a lo dispuesto en la legislación sobre contratación del sector público. El titular del máximo órgano de dirección del organismo autónomo será el órgano de contratación.

Artículo 101. *Régimen económico-financiero y patrimonial.*

1. Los organismos autónomos tendrán, para el cumplimiento de sus fines, un patrimonio propio, distinto del de la Administración Pública, integrado por el conjunto de bienes y derechos de los que sean titulares.

La gestión y administración de sus bienes y derechos propios, así como de aquellos del Patrimonio de la Administración que se les adscriban para el cumplimiento de sus fines, será ejercida de acuerdo a lo establecido para los organismos autónomos en la Ley 33/2003, de 3 de noviembre.

2. Los recursos económicos de los organismos autónomos podrán provenir de las siguientes fuentes:

a) Los bienes y valores que constituyen su patrimonio.

b) Los productos y rentas de dicho patrimonio.

c) Las consignaciones específicas que tuvieren asignadas en los presupuestos generales del Estado.

d) Las transferencias corrientes o de capital que procedan de la Administración o entidades públicas.

e) Las donaciones, legados, patrocinios y otras aportaciones de entidades privadas y de particulares.

f) Cualquier otro recurso que estén autorizados a percibir, según las disposiciones por las que se rijan o que pudieran serles atribuidos.

Artículo 102. *Régimen presupuestario, de contabilidad y control económico-financiero.*

Los organismo autónomos aplicarán el régimen presupuestario, económico-financiero, de contabilidad, y de control establecido por la Ley 47/2003, de 26 de noviembre.

Sección 3.ª Las entidades públicas empresariales de ámbito estatal

Artículo 103. *Definición.*

1. Las entidades públicas empresariales son entidades de Derecho público, con personalidad jurídica propia, patrimonio propio y autonomía en su gestión, que se financian con ingresos de mercado, a excepción de aquellas que tengan la condición o reúnan los requisitos para ser declaradas medio propio personificado de conformidad con la Ley de Contratos del Sector Público, y que junto con el ejercicio de potestades administrativas desarrollan actividades prestacionales, de gestión de servicios o de producción de bienes de interés público, susceptibles de contraprestación.

2. Las entidades públicas empresariales dependen de la Administración General del Estado o de un Organismo autónomo vinculado o dependiente de ésta, al que le corresponde la dirección estratégica, la evaluación de los resultados de su actividad y el control de eficacia.

3. Con independencia de cuál sea su denominación, cuando un organismo público tenga naturaleza jurídica de entidad pública empresarial deberá figurar en su denominación la indicación de «entidad pública empresarial» o su abreviatura «E.P.E».

Artículo 104. *Régimen jurídico.*

Las entidades públicas empresariales se rigen por el Derecho privado, excepto en la formación de la voluntad de sus órganos, en el ejercicio de las potestades administrativas que tengan atribuidas y en los aspectos específicamente regulados para las mismas en esta Ley, en su Ley de creación, sus estatutos, la Ley de Procedimiento Administrativo Común, el Real Decreto Legislativo 3/2011, de 14 de noviembre, la Ley 33/2003, de 3 de noviembre, y el resto de normas de derecho administrativo general y especial que le sean de aplicación.

Artículo 105. *Ejercicio de potestades administrativas.*

1. Las potestades administrativas atribuidas a las entidades públicas empresariales sólo pueden ser ejercidas por aquellos órganos de éstas a los que los estatutos se les asigne expresamente esta facultad.

2. No obstante, a los efectos de esta Ley, los órganos de las entidades públicas empresariales no son asimilables en cuanto a su rango administrativo al de los órganos de la Administración General del Estado, salvo las excepciones que, a determinados efectos se fijen, en cada caso, en sus estatutos.

Artículo 106. *Régimen jurídico del personal y de contratación.*

1. El personal de las entidades públicas empresariales se rige por el Derecho laboral, con las especificaciones dispuestas en este artículo y las excepciones relativas a los funcionarios públicos de la Administración General del Estado, quienes se regirán por lo previsto en la Ley 7/2007, de 12 de abril y demás normativa reguladora de los funcionarios públicos o por la normativa laboral.

2. La selección del personal laboral de estas entidades se realizará conforme a las siguientes reglas:

a) El personal directivo, que se determinará en los estatutos de la entidad, será nombrado con arreglo a los criterios establecidos en el apartado 11 del artículo 55, atendiendo a la experiencia en el desempeño de puestos de responsabilidad en la gestión pública o privada.

b) El resto del personal será seleccionado mediante convocatoria pública basada en los principios de igualdad, mérito y capacidad.

3. **(Suprimido)**

4. El Ministerio de Hacienda y Administraciones Públicas efectuará, con la periodicidad adecuada, controles específicos sobre la evolución de los gastos de personal y de la gestión de sus recursos humanos, conforme a los criterios previamente establecidos por los mismos.

5. La Ley de creación de cada entidad pública empresarial deberá determinar las condiciones conforme a las cuales, los funcionarios de la Administración General del Estado,

podrán cubrir destinos en la referida entidad, y establecerá, asimismo, las competencias que a la misma correspondan sobre este personal que, en todo caso, serán las que tengan legalmente atribuidas los Organismos autónomos.

6. La contratación de las entidades públicas empresariales se rige por las previsiones contenidas al respecto en la legislación de contratos del sector público.

Artículo 107. *Régimen económico-financiero y patrimonial.*

1. Las entidades públicas empresariales tendrán, para el cumplimiento de sus fines, un patrimonio propio, distinto del de la Administración Pública, integrado por el conjunto de bienes y derechos de los que sean titulares.

La gestión y administración de sus bienes y derechos propios, así como de aquellos del Patrimonio de la Administración que se les adscriban para el cumplimiento de sus fines, será ejercida de acuerdo con lo previsto en la Ley 33/2003, de 3 de noviembre.

2. Las entidades públicas empresariales podrán financiarse con los ingresos que se deriven de sus operaciones, obtenidos como contraprestación de sus actividades comerciales, y con los recursos económicos que provengan de las siguientes fuentes:

a) Los bienes y valores que constituyen su patrimonio.

b) Los productos y rentas de dicho patrimonio y cualquier otro recurso que pudiera serle atribuido.

Excepcionalmente, cuando así lo prevea la Ley de creación, podrá financiarse con los recursos económicos que provengan de las siguientes fuentes:

a) Las consignaciones específicas que tuvieran asignadas en los Presupuestos Generales del Estado.

b) Las transferencias corrientes o de capital que procedan de las Administraciones o entidades públicas.

c) Las donaciones, legados, patrocinios y otras aportaciones de entidades privadas y de particulares.

3. Las entidades público empresariales se financiarán mayoritariamente con ingresos de mercado, a excepción de aquellas que tengan la condición o reúnan los requisitos para ser declaradas medio propio personificado de conformidad con la Ley de Contratos del Sector Público. Se entiende que se financian mayoritariamente con ingresos de mercado cuando tengan la consideración de productor de mercado de conformidad con el Sistema Europeo de Cuentas.

A tales efectos se tomará en consideración la clasificación de las diferentes entidades públicas a los efectos de la contabilidad nacional que efectúe el Comité Técnico de Cuentas Nacionales y que se recogerá en el Inventario de Entidades del sector Público estatal, Autonómico y Local.

Artículo 108. *Régimen presupuestario, de contabilidad y control económico-financiero.*

Las entidades públicas empresariales aplicarán el régimen presupuestario, económico-financiero, de contabilidad y de control establecido en la Ley 47/2003, de 26 de noviembre.

Sección 4.ª Agencias estatales

Artículo 108 bis. *Definición.*

1. Las Agencias Estatales son entidades de derecho público, dotadas de personalidad jurídica pública, patrimonio propio y autonomía en su gestión, facultadas para ejercer potestades administrativas, que son creadas por el Gobierno para el cumplimiento de los programas correspondientes a las políticas públicas que desarrolle la Administración General del Estado en el ámbito de sus competencias.

Las agencias estatales están dotadas de los mecanismos de autonomía funcional, responsabilidad por la gestión y control de resultados establecidos en esta ley.

2. Con independencia de cuál sea su denominación, cuando un organismo público tenga naturaleza de Agencia Estatales deberá figurar en su denominación la indicación de "Agencia Estatal".

Artículo 108 ter. *Régimen jurídico.*

1. Las agencias estatales se rigen por esta ley y, en su marco, por el estatuto propio de cada una de ellas; y el resto de las normas de derecho administrativo general y especial que le sea de aplicación.

2. La actuación de las agencias estatales se produce, con arreglo al plan de acción anual, bajo la vigencia y con arreglo al pertinente contrato plurianual de gestión que ha de establecer, como mínimo y para el periodo de su vigencia, los siguientes extremos:

a) Los objetivos a perseguir, los resultados a obtener y, en general, la gestión a desarrollar.

b) Los planes necesarios para alcanzar los objetivos, con especificación de los marcos temporales correspondientes y de los proyectos asociados a cada una de las estrategias y sus plazos temporales, así como los indicadores para evaluar los resultados obtenidos.

c) Las previsiones máximas de plantilla de personal y el marco de actuación en materia de gestión de recursos humanos.

d) Los recursos personales, materiales y presupuestarios a aportar para la consecución de los objetivos, si bien serán automáticamente revisados de conformidad con el contenido de la Ley de Presupuestos Generales del Estado del ejercicio correspondiente.

e) Los efectos asociados al grado de cumplimiento de los objetivos establecidos por lo que hace a exigencia de responsabilidad por la gestión de los órganos ejecutivos y el personal directivo, así como el montante de masa salarial destinada al complemento de productividad o concepto equivalente del personal laboral.

f) El procedimiento a seguir para la cobertura de los déficits anuales que, en su caso, se pudieran producir por insuficiencia de los ingresos reales respecto de los estimados y las consecuencias de responsabilidad en la gestión que, en su caso, deban seguirse de tales déficits. Dicho procedimiento deberá ajustarse, en todo caso, a lo que establezca el contenido de la Ley de Presupuestos Generales del Estado del ejercicio correspondiente.

g) El procedimiento para la introducción de las modificaciones o adaptaciones anuales que, en su caso, procedan.

3. En el contrato de gestión se determinarán los mecanismos que permitan la exigencia de responsabilidades a que se refiere la letra e) del apartado anterior por incumplimiento de objetivos.

4. El Consejo Rector de cada agencia estatal aprueba la propuesta de contrato inicial de gestión, en el plazo de tres meses desde su constitución.

Los posteriores contratos de gestión se presentarán en el último trimestre de la vigencia del anterior.

La aprobación del contrato de gestión tiene lugar por Orden conjunta de los Ministerios de adscripción, de Política Territorial y Función Pública y de Hacienda, en un plazo máximo de tres meses a contar desde su presentación. En el caso de no ser aprobado en este plazo mantendrá su vigencia el contrato de gestión anterior.

5. En el seno del Consejo Rector se constituirá una Comisión de Control, con la composición que se determine en los estatutos.

Corresponde a la Comisión de Control informar al Consejo Rector sobre la ejecución del contrato de gestión y, en general, sobre todos aquellos aspectos relativos a la gestión económico-financiera que deba conocer el propio Consejo y que se determinen en los Estatutos.

Artículo 108 quater. *Régimen jurídico de personal.*

1. El personal al servicio de las Agencias Estatales está constituido por:

a) El personal que esté ocupando puestos de trabajo en servicios que se integren en la Agencia Estatal en el momento de su constitución.

b) El personal que se incorpore a la Agencia Estatal desde cualquier administración pública por los correspondientes procedimientos de provisión de puestos de trabajo previstos en esta ley.

c) El personal seleccionado por la Agencia Estatal, mediante pruebas selectivas convocadas al efecto en los términos establecidos en esta Ley.

d) El personal directivo.

2. El personal a que se refieren las letras a) y b) del apartado anterior mantiene la condición de personal funcionario, estatutario o laboral de origen, de acuerdo con la legislación aplicable.

3. El personal funcionario y estatutario se rige por la normativa reguladora de la función pública correspondiente, con las especialidades previstas en esta Ley y las que, conforme a ella, se establezcan en el estatuto de cada agencia estatal.

El personal laboral se rige por el Texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, y el resto de la normativa laboral.

4. La selección del personal al que se refiere la letra c) se realiza mediante convocatoria pública y de acuerdo con los principios de igualdad, mérito y capacidad, así como de acceso al empleo público de las personas con discapacidad. A tal efecto, y en el período previsto en el contrato de gestión, las agencias estatales determinan sus necesidades de personal a cubrir mediante pruebas selectivas. La determinación de las necesidades de personal a cubrir se realizará con sujeción a la tasa de reposición que, en su caso, se establezca en la Ley de Presupuestos Generales del Estado para el ejercicio correspondiente. La previsión de necesidades de personal se incorpora a la oferta anual de empleo de la correspondiente agencia estatal, que se integra en la oferta de empleo público estatal, de conformidad con lo que establezca la Ley anual de Presupuestos Generales del Estado.

Las agencias estatales seleccionan a través de sus propios órganos de selección, a su personal laboral de acuerdo con los requisitos y principios establecidos en el párrafo anterior.

Las convocatorias de selección de personal funcionario se efectuarán por el Ministerio al que se encuentren adscritos los cuerpos o escalas correspondientes, y, excepcionalmente por la propia agencia estatal mediante convenio suscrito al efecto.

Los órganos de representación del personal de la agencia estatal serán tenidos en cuenta en los procesos de selección que se lleven a cabo.

5. Las agencias estatales elaboran, convocan y, a propuesta de órganos especializados en selección de personal, resuelven las correspondientes convocatorias de provisión de puestos de trabajo de personal funcionario, de conformidad con los principios generales y procedimientos de provisión establecidos en la normativa de función pública.

6. La movilidad de los funcionarios destinados en las agencias estatales podrá estar sometida a la condición de autorización previa en las condiciones y con los plazos que se determinen en sus estatutos y de acuerdo con la normativa de función pública.

7. Las agencias estatales disponen de su relación de puestos de trabajo, elaborada y aprobada por la propia agencia estatal dentro del marco de actuación que, en materia de recursos humanos, se establezca en el contrato de gestión.

8. El personal que preste sus servicios en las agencias estatales verá reconocido su derecho a la promoción dentro de una carrera profesional evaluable, en el marco del Estatuto del Empleado Público. Dicha carrera tendrá elementos que permitan criterios de homogeneidad dentro de agencias estatales del mismo ámbito, facilitando similares retribuciones para niveles profesionales semejantes y posibilitando las medidas de movilidad entre el personal de aquellas, sin perjuicio de lo previsto en el apartado 6.

9. Los conceptos retributivos del personal funcionario y estatutario de las agencias estatales, son los establecidos en la normativa de función pública de la Administración General del Estado y sus cuantías se determinarán de conformidad con lo establecido en las Leyes de Presupuestos Generales del Estado.

Las condiciones retributivas del personal laboral son las determinadas en el convenio colectivo de aplicación y en el respectivo contrato de trabajo y sus cuantías se fijarán de acuerdo con lo indicado en el apartado 1 anterior.

La masa salarial de las agencias estatales se autorizará en las condiciones que establezca la normativa aplicable. La cuantía de la masa salarial destinada al complemento

de productividad, o concepto equivalente del personal laboral, está en todo caso vinculada al grado de cumplimiento de los objetivos fijados en el contrato de gestión.

10. El personal directivo de las agencias estatales es el que ocupa los puestos de trabajo determinados como tales en el estatuto de las mismas en atención a la especial responsabilidad, competencia técnica y relevancia de las tareas a ellos asignadas.

El personal directivo de las agencias estatales es nombrado y cesado por su Consejo Rector a propuesta de sus órganos ejecutivos, atendiendo a criterios de competencia profesional y experiencia entre titulados superiores preferentemente funcionarios, y mediante procedimiento que garantice el mérito, la capacidad y la publicidad.

El proceso de provisión podrá ser realizado por los órganos de selección especializados a los que se refiere el apartado 5 de este artículo, que formularán propuesta motivada al director de la agencia estatal, incluyendo tres candidatos para cada puesto a cubrir.

Cuando el personal directivo de las agencias estatales tenga la condición de funcionario permanecerá en la situación de servicio activo en su respectivo cuerpo o escala o en la que corresponda con arreglo a la legislación laboral si se trata de personal de este carácter.

El estatuto de las agencias estatales puede prever puestos directivos de máxima responsabilidad a cubrir, en régimen laboral, mediante contratos de alta dirección.

Al personal directivo de las agencias estatales, en todo caso, le será de aplicación el Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos en el sector público empresarial y otras entidades. El personal directivo está sujeto, en el desarrollo de sus cometidos, a evaluación con arreglo a los criterios de eficacia, eficiencia y cumplimiento de la legalidad, responsabilidad por su gestión y control de resultados en relación con los objetivos que le hayan sido fijados.

El personal directivo percibe una parte de su retribución como incentivo de rendimiento, mediante el complemento correspondiente que valore la productividad, de acuerdo con los criterios y porcentajes que se establezcan por el Consejo Rector, a propuesta de los órganos directivos de la Agencia Estatal.

11. El órgano ejecutivo de la agencia estatal es el director. Es nombrado y separado por el Consejo Rector a propuesta del Presidente entre personas que reúnan las cualificaciones necesarias para el cargo, según se determine en el Estatuto.

Artículo 108 quinquies. *Régimen económico financiero y contratación.*

1. Las Agencias Estatales se financian con los siguientes recursos:

a) Las transferencias consignadas en los Presupuestos Generales del Estado.

b) Los ingresos propios que perciba como contraprestación por las actividades que pueda realizar, en virtud de contratos, convenios o disposición legal, para otras entidades públicas, privadas o personas físicas.

c) La enajenación de los bienes y valores que constituyan su patrimonio.

d) El rendimiento procedente de sus bienes y valores.

e) Las aportaciones voluntarias, donaciones, herencias y legados y otras aportaciones a título gratuito de entidades privadas y de particulares.

f) Los ingresos recibidos de personas físicas o jurídicas como consecuencia del patrocinio de actividades o instalaciones.

g) Los demás ingresos de derecho público o privado que estén autorizadas a percibir.

h) Cualquier otro recurso que pudiera serles atribuido.

2. En aquellos supuestos expresamente previstos en los estatutos, y solo en la medida que tengan capacidad para generar recursos propios suficientes, las Agencias Estatales podrán financiarse con cargo a los créditos previstos en el capítulo VIII de los Presupuestos Generales del Estado adjudicados de acuerdo con procedimientos de pública concurrencia y destinados a financiar proyectos de investigación y desarrollo. La Ley de Presupuestos Generales del Estado de cada ejercicio establecerá los límites de esta financiación.

3. Los recursos que se deriven de los apartados b), e), f) y g) del número 1 anterior, y no se contemplen inicialmente en el presupuesto de las Agencias Estatales se podrán destinar a financiar mayores gastos por acuerdo de su Director.

4. El recurso al endeudamiento está prohibido a las agencias estatales, salvo que por Ley se disponga lo contrario. No obstante, y con objeto de atender desfases temporales de

tesorería, las agencias estatales pueden recurrir a la contratación de pólizas de crédito o préstamo, siempre que el saldo vivo no supere el 5 % de su presupuesto.

5. La contratación de las agencias estatales se rige por la normativa aplicable al sector público. Las sociedades mercantiles y fundaciones creadas o participadas mayoritariamente por las agencias estatales, deberán ajustar su actividad contractual, en todo caso, a los principios de publicidad y concurrencia.

Artículo 108 sexies. *Régimen presupuestario, de contabilidad y control económico financiero.*

1. El Consejo Rector elaborará y aprobará el anteproyecto de presupuesto de la agencia estatal, conforme a lo dispuesto en el contrato de gestión. El anteproyecto de presupuesto de la agencia estatal será remitido al Ministerio de adscripción para su examen, que dará posterior traslado del mismo al Ministerio de Hacienda. Una vez analizado por este último departamento ministerial, el anteproyecto se incorpora al de Presupuestos Generales del Estado para su aprobación por el Consejo de Ministros y remisión a las Cortes Generales, consolidándose con el de las restantes entidades que integran el sector público estatal.

2. La persona titular del Ministerio de Hacienda establece la estructura del presupuesto de las agencias estatales, así como la documentación que se debe acompañar al mismo.

El presupuesto de gastos de las agencias estatales, tiene carácter limitativo por su importe global y carácter estimativo para la distribución de los créditos en categorías económicas, con excepción de los correspondientes a gastos de personal que en todo caso tienen carácter limitativo y vinculante por su cuantía total, y de las subvenciones nominativas y las atenciones protocolarias y representativas que tendrán carácter limitativo y vinculante cualquiera que sea el nivel de la clasificación económica al que se establezcan.

3. La autorización de las variaciones presupuestarias corresponde:

a) A la persona titular del Ministerio de Hacienda, las variaciones de la cuantía global del presupuesto y las que afecten a gastos de personal, a iniciativa del director y propuesta del Consejo Rector, salvo las previstas en la letra siguiente.

Así mismo, corresponde a la persona titular del Ministerio de Hacienda acordar o denegar las modificaciones presupuestarias, en los supuestos de competencia de los directores de las agencias estatales, cuando exista informe negativo de la Intervención Delegada y el titular de la competencia lo remita en discrepancia al Ministro Hacienda.

b) A la persona titular de la Dirección de la propia agencia estatal, todas las restantes variaciones, incluso en la cuantía global cuando sean financiadas con recursos derivados de los apartados b), e), f), y g) del artículo 108 quinquies por encima de los inicialmente presupuestados, no afecten a gastos de personal y existan garantías suficientes de su efectividad, dando cuenta inmediata a la Comisión de Control.

4. Los remanentes de tesorería que resulten de la liquidación del ejercicio presupuestario no afectados a la financiación del presupuesto del ejercicio siguiente, podrán aplicarse al presupuesto de ingresos y destinarse a financiar incremento de gastos por acuerdo de la persona titular de la Dirección, dando cuenta a la Comisión de Control. Los déficits derivados del incumplimiento de la estimación de ingresos anuales se compensarán en la forma que se prevea en el contrato de gestión.

5. Las agencias estatales podrán adquirir compromisos de gasto que hayan de extenderse a ejercicios posteriores a aquel en que se autoricen, siempre que no se superen alguno de los siguientes límites:

a) El número de ejercicios a que pueden aplicarse los gastos no será superior a cuatro.

b) El gasto que se impute a cada uno de los ejercicios posteriores no podrá exceder de la cantidad que resulte de aplicar al importe total de cada programa, excluido el capítulo de gastos de personal y los restantes créditos que tengan carácter vinculante, los siguientes porcentajes: El 70 por 100 en el ejercicio inmediato siguiente, el 60 por ciento en el segundo ejercicio y el 50 por ciento en los ejercicios tercero y cuarto.

En el caso de gastos de personal o de otros que tengan carácter vinculante, podrán adquirirse compromisos de gasto con cargo a ejercicios futuros dentro de los límites señalados anteriormente, tomando como referencia de cálculo su dotación inicial.

El Gobierno podrá acordar la modificación de los límites anteriores en los casos especialmente justificados. A estos efectos, la persona titular del Ministerio de Hacienda, a iniciativa de la agencia estatal correspondiente, elevará al Consejo de Ministros la oportuna propuesta, previo informe de la Dirección General de Presupuestos.

6. La ejecución del presupuesto de las agencias estatales corresponde a sus órganos ejecutivos, que elaboran y remiten a la Comisión de Control, mensualmente, un estado de ejecución presupuestaria.

7. Las agencias estatales deberán aplicar los principios contables que les corresponda de acuerdo con lo establecido en el artículo 121 de la Ley General Presupuestaria, con la finalidad de asegurar el adecuado reflejo de las operaciones, los costes y los resultados de su actividad, así como de facilitar datos e información con trascendencia económica.

Corresponde a la Intervención General de la Administración del Estado establecer los criterios que precise la aplicación de la normativa contable a las agencias estatales, en los términos establecidos por la legislación presupuestaria para las entidades del sector público estatal.

8. Las agencias estatales dispondrán de:

a) Un sistema de información económica que:

i) Muestre, a través de estados e informes, la imagen fiel del patrimonio, de la situación financiera, de los resultados y de la ejecución del presupuesto.

ii) Proporcione información de costes sobre su actividad que sea suficiente para una correcta y eficiente adopción de decisiones.

b) Un sistema de contabilidad de gestión que permita efectuar el seguimiento del cumplimiento de los compromisos asumidos en el contrato de gestión.

La Intervención General de la Administración del Estado establece los requerimientos funcionales y, en su caso, los procedimientos informáticos, que deberán observar las agencias estatales para cumplir lo dispuesto en este artículo, de acuerdo con lo dispuesto en el artículo 125 de la Ley General Presupuestaria.

9. Las cuentas anuales de las agencias estatales se formulan por la persona titular de la Dirección en el plazo de tres meses desde el cierre del ejercicio económico. Una vez auditadas dichas cuentas por la Intervención General de la Administración del Estado son sometidas al Consejo Rector, para su aprobación antes del 30 de junio del año siguiente al que se refieran.

Una vez aprobadas por el Consejo Rector, las cuentas se remitirán a través de la Intervención General de la Administración del Estado al Tribunal de Cuentas para su fiscalización. Dicha remisión a la Intervención General se realizará dentro de los siete meses siguientes a la terminación del ejercicio económico.

10. El control externo de la gestión económico-financiera de las agencias estatales corresponde al Tribunal de Cuentas de acuerdo con su normativa específica.

El control interno de la gestión económico-financiera de las agencias estatales corresponde a la Intervención General de la Administración del Estado, y se realizará bajo las modalidades de control financiero permanente y de auditoría pública, en las condiciones y en los términos establecidos en la Ley General Presupuestaria. El control financiero permanente se realizará por las Intervenciones Delegadas en las Agencias Estatales, bajo la dependencia funcional de la Intervención General de la Administración del Estado.

Sin perjuicio del control establecido en el párrafo anterior, las agencias estatales estarán sometidas a un control de eficacia y de supervisión continua que será ejercido, a través del seguimiento del contrato de gestión y hasta su aprobación a través del plan de actuación en los términos establecidos en el artículo 85.

CAPÍTULO IV

Las autoridades administrativas independientes de ámbito estatal

Artículo 109. *Definición.*

1. Son autoridades administrativas independientes de ámbito estatal las entidades de derecho público que, vinculadas a la Administración General del Estado y con personalidad jurídica propia, tienen atribuidas funciones de regulación o supervisión de carácter externo sobre sectores económicos o actividades determinadas, por requerir su desempeño de independencia funcional o una especial autonomía respecto de la Administración General del Estado, lo que deberá determinarse en una norma con rango de Ley.

2. Las autoridades administrativas independientes actuarán, en el desarrollo de su actividad y para el cumplimiento de sus fines, con independencia de cualquier interés empresarial o comercial.

3. Con independencia de cuál sea su denominación, cuando una entidad tenga la naturaleza jurídica de autoridad administrativa independiente deberá figurar en su denominación la indicación «autoridad administrativa independiente» o su abreviatura «A.A.I.».

Artículo 110. *Régimen jurídico.*

1. Las autoridades administrativas independientes se regirán por su Ley de creación, sus estatutos y la legislación especial de los sectores económicos sometidos a su supervisión y, supletoriamente y en cuanto sea compatible con su naturaleza y autonomía, por lo dispuesto en esta Ley, en particular lo dispuesto para organismos autónomos, la Ley del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 47/2003, de 26 de noviembre, el Real Decreto Legislativo 3/2011, de 14 de noviembre, la Ley 33/2003, de 3 de noviembre, así como el resto de las normas de derecho administrativo general y especial que le sea de aplicación. En defecto de norma administrativa, se aplicará el derecho común.

2. Las autoridades administrativas independientes estarán sujetas al principio de sostenibilidad financiera de acuerdo con lo previsto en la Ley Orgánica 2/2012, de 27 de abril.

CAPÍTULO V

De las sociedades mercantiles estatales

Artículo 111. *Definición.*

1. Se entiende por sociedad mercantil estatal aquella sociedad mercantil sobre la que se ejerce control estatal:

a) Bien porque la participación directa, en su capital social de la Administración General del Estado o alguna de las entidades que, conforme a lo dispuesto en el artículo 84, integran el sector público institucional estatal, incluidas las sociedades mercantiles estatales, sea superior al 50 por 100. Para la determinación de este porcentaje, se sumarán las participaciones correspondientes a la Administración General del Estado y a todas las entidades integradas en el sector público institucional estatal, en el caso de que en el capital social participen varias de ellas.

b) Bien porque la sociedad mercantil se encuentre en el supuesto previsto en el artículo 4 de la Ley 24/1988, de 28 de julio, del Mercado de Valores respecto de la Administración General del Estado o de sus organismos públicos vinculados o dependientes.

2. En la denominación de las sociedades mercantiles que tengan la condición de estatales deberá figurar necesariamente la indicación «sociedad mercantil estatal» o su abreviatura «S.M.E.».

Artículo 112. *Principios rectores.*

La Administración General del Estado y las entidades integrantes del sector público institucional, en cuanto titulares del capital social de las sociedades mercantiles estatales, perseguirán la eficiencia, transparencia y buen gobierno en la gestión de dichas sociedades mercantiles, para lo cual promoverán las buenas prácticas y códigos de conducta adecuados a la naturaleza de cada entidad. Todo ello sin perjuicio de la supervisión general que ejercerá el accionista sobre el funcionamiento de la sociedad mercantil estatal, conforme prevé la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.

Artículo 113. *Régimen jurídico.*

Las sociedades mercantiles estatales se regirán por lo previsto en esta Ley, por lo previsto en la Ley 33/2003, de 3 de noviembre, y por el ordenamiento jurídico privado, salvo en las materias en que le sea de aplicación la normativa presupuestaria, contable, de personal, de control económico-financiero y de contratación. En ningún caso podrán disponer de facultades que impliquen el ejercicio de autoridad pública, sin perjuicio de que excepcionalmente la ley pueda atribuirle el ejercicio de potestades administrativas.

Artículo 114. *Creación y extinción.*

1. La creación de una sociedad mercantil estatal o la adquisición de este carácter de forma sobrevenida será autorizada mediante acuerdo del Consejo de Ministros que deberá ser acompañado de una propuesta de estatutos y de un plan de actuación que contendrá, al menos:

a) Las razones que justifican la creación de la sociedad por no poder asumir esas funciones otra entidad ya existente, así como la inexistencia de duplicidades. A estos efectos, deberá dejarse constancia del análisis realizado sobre la existencia de órganos o entidades que desarrollan actividades análogas sobre el mismo territorio y población y las razones por las que la creación de la nueva sociedad no entraña duplicidad con entidades existentes.

b) Un análisis que justifique que la forma jurídica propuesta resulta más eficiente frente a la creación de un organismo público u otras alternativas de organización que se hayan descartado.

c) Los objetivos anuales y los indicadores para medirlos.

Al acuerdo de creación de la sociedad mercantil estatal se acompañará un informe preceptivo favorable del Ministerio de Hacienda y Administraciones Públicas o la Intervención General de la Administración del Estado, según se determine reglamentariamente, que valorará el cumplimiento de lo previsto en este artículo.

El Programa de Actuación Plurianual que conforme a la Ley 47/2003, de 26 de noviembre, deben elaborar las sociedades cada año incluirá un plan de actuación anual que servirá de base para el control de eficacia de la sociedad. La falta de aprobación del plan de actuación dentro del plazo anual fijado, por causa imputable a la sociedad y hasta tanto se subsane la omisión, llevará aparejada la paralización de las aportaciones que deban realizarse a favor de la sociedad con cargo a los presupuestos generales del Estado.

2. La liquidación de una sociedad mercantil estatal recaerá en un órgano de la Administración General del Estado o en una entidad integrante del sector público institucional estatal.

La responsabilidad que le corresponda al empleado público como miembro de la entidad u órgano liquidador será directamente asumida por la entidad o la Administración General del Estado que lo designó, quien podrá exigir de oficio al empleado público la responsabilidad que, en su caso, corresponda cuando concurra dolo, culpa o negligencia grave conforme a lo previsto en las leyes administrativas en materia de responsabilidad patrimonial.

Artículo 115. *Régimen de responsabilidad aplicable a los miembros de los consejos de administración de las sociedades mercantiles estatales designados por la Administración General del Estado.*

1. La responsabilidad que le corresponda al empleado público como miembro del consejo de administración será directamente asumida por la Administración General del Estado que lo designó.

2. La Administración General del Estado podrá exigir de oficio al empleado público que designó como miembro del consejo de administración la responsabilidad en que hubiera incurrido por los daños y perjuicios causados en sus bienes o derechos cuando hubiera concurrido dolo, o culpa o negligencia graves, conforme a lo previsto en las leyes administrativas en materia de responsabilidad patrimonial.

Artículo 116. *Tutela.*

1. Al autorizar la constitución de una sociedad mercantil estatal con forma de sociedad anónima, de acuerdo con lo previsto en el artículo 166.2 de la Ley 33/2003, de 3 de noviembre, el Consejo de Ministros podrá atribuir a un Ministerio, cuyas competencias guarden una relación específica con el objeto social de la sociedad, la tutela funcional de la misma.

2. En ausencia de esta atribución expresa corresponderá íntegramente al Ministerio de Hacienda y Administraciones Públicas el ejercicio de las facultades que esta Ley y la Ley 33/2003, de 3 de noviembre, otorgan para la supervisión de la actividad de la sociedad.

3. El Ministerio de tutela ejercerá el control de eficacia e instruirá a la sociedad respecto a las líneas de actuación estratégica y establecerá las prioridades en la ejecución de las mismas, y propondrá su incorporación a los Presupuestos de Explotación y Capital y Programas de Actuación Plurianual, previa conformidad, en cuanto a sus aspectos financieros, de la Dirección General del Patrimonio del Estado si se trata de sociedades cuyo capital corresponda íntegramente a la Administración General del Estado, o del organismo público que sea titular de su capital.

4. En casos excepcionales, debidamente justificados, el titular del departamento al que corresponda su tutela podrá dar instrucciones a las sociedades, para que realicen determinadas actividades, cuando resulte de interés público su ejecución.

5. Cuando las instrucciones que imparta el Ministerio de tutela impliquen una variación de los Presupuestos de Explotación y Capital de acuerdo con lo dispuesto en la Ley 47/2003, de 26 de noviembre, el órgano de administración no podrá iniciar la cumplimentación de la instrucción sin contar con la autorización del órgano competente para efectuar la modificación correspondiente.

6. En este caso, los administradores de las sociedades a las que se hayan impartido estas instrucciones actuarán diligentemente para su ejecución, y quedarán exonerados de la responsabilidad prevista en el artículo 236 del Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital, si del cumplimiento de dichas instrucciones se derivaren consecuencias lesivas.

Artículo 117. *Régimen presupuestario, de contabilidad, control económico-financiero y de personal.*

1. Las sociedades mercantiles estatales elaborarán anualmente un presupuesto de explotación y capital y un plan de actuación que forma parte del Programa Plurianual, que se integrarán con el Presupuesto General del Estado. El Programa contendrá la revisión trienal del plan de creación a que se refiere el artículo 85.

2. Las sociedades mercantiles estatales formularán y rendirán sus cuentas de acuerdo con los principios y normas de contabilidad recogidos en el Código de Comercio y el Plan General de Contabilidad y disposiciones que lo desarrollan.

3. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico financiera de las sociedades mercantiles estatales estará sometida al control de la Intervención General de la Administración del Estado.

4. El personal de las sociedades mercantiles estatales, incluido el que tenga condición de directivo, se regirá por el Derecho laboral, así como por las normas que le sean de

aplicación en función de su adscripción al sector público estatal, incluyendo siempre entre las mismas la normativa presupuestaria, especialmente lo que se establezca en las Leyes de Presupuestos Generales del Estado.

CAPÍTULO VI

De los consorcios

Artículo 118. *Definición y actividades propias.*

1. Los consorcios son entidades de derecho público, con personalidad jurídica propia y diferenciada, creadas por varias Administraciones Públicas o entidades integrantes del sector público institucional, entre sí o con participación de entidades privadas, para el desarrollo de actividades de interés común a todas ellas dentro del ámbito de sus competencias.

2. Los consorcios podrán realizar actividades de fomento, prestacionales o de gestión común de servicios públicos y cuantas otras estén previstas en las leyes.

3. Los consorcios podrán utilizarse para la gestión de los servicios públicos, en el marco de los convenios de cooperación transfronteriza en que participen las Administraciones españolas, y de acuerdo con las previsiones de los convenios internacionales ratificados por España en la materia.

4. En la denominación de los consorcios deberá figurar necesariamente la indicación «consorcio» o su abreviatura «C».

Artículo 119. *Régimen jurídico.*

1. Los consorcios se regirán por lo establecido en esta Ley, en la normativa autonómica de desarrollo y sus estatutos.

2. En lo no previsto en esta Ley, en la normativa autonómica aplicable, ni en sus Estatutos sobre el régimen del derecho de separación, disolución, liquidación y extinción, se estará a lo previsto en el Código Civil sobre la sociedad civil, salvo el régimen de liquidación, que se someterá a lo dispuesto en el artículo 97, y en su defecto, el Real Decreto Legislativo 1/2010, de 2 de julio.

3. Las normas establecidas en la Ley 7/1985, de 2 de abril, y en la Ley 27/2013, de 21 de diciembre, de racionalización y sostenibilidad de la Administración Local sobre los Consorcios locales tendrán carácter supletorio respecto a lo dispuesto en esta Ley.

Artículo 120. *Régimen de adscripción.*

1. Los estatutos de cada consorcio determinarán la Administración Pública a la que estará adscrito de conformidad con lo previsto en este artículo.

2. De acuerdo con los siguientes criterios, ordenados por prioridad en su aplicación y referidos a la situación en el primer día del ejercicio presupuestario, el consorcio quedará adscrito, en cada ejercicio presupuestario y por todo este periodo, a la Administración Pública que:

a) Disponga de la mayoría de votos en los órganos de gobierno.

b) Tenga facultades para nombrar o destituir a la mayoría de los miembros de los órganos ejecutivos.

c) Tenga facultades para nombrar o destituir a la mayoría de los miembros del personal directivo.

d) Disponga de un mayor control sobre la actividad del consorcio debido a una normativa especial.

e) Tenga facultades para nombrar o destituir a la mayoría de los miembros del órgano de gobierno.

f) Financie en más de un cincuenta por ciento, en su defecto, en mayor medida la actividad desarrollada por el consorcio, teniendo en cuenta tanto la aportación del fondo patrimonial como la financiación concedida cada año.

g) Ostente el mayor porcentaje de participación en el fondo patrimonial.

h) Tenga mayor número de habitantes o extensión territorial dependiendo de si los fines definidos en el estatuto están orientados a la prestación de servicios a las personas, o al desarrollo de actuaciones sobre el territorio.

3. En el supuesto de que participen en el consorcio entidades privadas, el consorcio no tendrá ánimo de lucro y estará adscrito a la Administración Pública que resulte de acuerdo con los criterios establecidos en el apartado anterior.

4. Cualquier cambio de adscripción a una Administración Pública, cualquiera que fuere su causa, conllevará la modificación de los estatutos del consorcio en un plazo no superior a seis meses, contados desde el inicio del ejercicio presupuestario siguiente a aquel en se produjo el cambio de adscripción.

Artículo 121. *Régimen de personal.*

El personal al servicio de los consorcios podrá ser funcionario o laboral y habrá de proceder de las Administraciones participantes, en cuyo caso su régimen jurídico será el de la Administración Pública de adscripción y sus retribuciones en ningún caso podrán superar las establecidas para puestos de trabajo equivalentes en aquella.

Excepcionalmente, cuando no resulte posible contar con personal procedente de las Administraciones participantes en el consorcio en atención a la singularidad de las funciones a desempeñar o cuando, tras un anuncio público de convocatoria para la cobertura de un puesto de trabajo restringida a las administraciones consorciadas, no fuera posible cubrir dicho puesto, el Ministerio de Hacienda y Función Pública, u órgano competente de la Administración a la que se adscriba el consorcio, podrá autorizar la contratación de personal por parte del consorcio para el ejercicio de dichas funciones, en los términos previstos en la correspondiente Ley de Presupuestos Generales del Estado.

Artículo 122. *Régimen presupuestario, de contabilidad, control económico-financiero y patrimonial.*

1. Los consorcios estarán sujetos al régimen de presupuestación, contabilidad y control de la Administración Pública a la que estén adscritos, sin perjuicio de su sujeción a lo previsto en la Ley Orgánica 2/2012, de 27 de abril.

2. A efectos de determinar la financiación por parte de las Administraciones consorciadas, se tendrán en cuenta tanto los compromisos estatutarios o convencionales existentes como la financiación real, mediante el análisis de los desembolsos efectivos de todas las aportaciones realizadas.

3. El órgano de control interno de la Administración a la que se haya adscrito el consorcio, deberá realizar la auditoría de cuentas anuales de aquellos consorcios en los que, a fecha de cierre del ejercicio, concurran, al menos, dos de las tres circunstancias siguientes:

a) Que el total de las partidas del activo supere 2.400.000 euros.

b) Que el importe total de sus ingresos por gestión ordinaria en el caso de los consorcios del sector público administrativo, o la suma del importe de la cifra de negocios más otros ingresos de gestión, en el caso de los pertenecientes al sector público empresarial, sea superior a 2.400.000 euros.

c) Que el número medio de trabajadores empleados durante el ejercicio sea superior a 50.

Mediante Ley, podrán modificarse los límites anteriores cuando la estructura y composición de los consorcios adscritos a una administración así lo requiera.

Las circunstancias señaladas anteriormente se aplicarán teniendo en cuenta lo siguiente:

a) Cuando un consorcio, en la fecha de cierre del ejercicio, pase a cumplir dos de las citadas circunstancias, o bien cese de cumplirlas, tal situación únicamente producirá efectos en cuanto a lo señalado si se repite durante dos ejercicios consecutivos.

b) En el primer ejercicio económico desde su constitución o su adscripción al sector público correspondiente, los consorcios cumplirán lo dispuesto en los apartados anteriormente mencionados si reúnen, al cierre de dicho ejercicio, al menos dos de las tres circunstancias que se señalan.

c) Aun cuando, según las circunstancias señaladas, no exista obligación de someter las cuentas anuales de un consorcio a auditoría de cuentas, los órganos de control interno podrán, en todo caso, incluir su realización en sus planes anuales de control y auditoría.

4. Los consorcios deberán formar parte de los presupuestos e incluirse en la cuenta general de la Administración Pública de adscripción.

5. Los consorcios se regirán por las normas patrimoniales de la Administración Pública a la que estén adscritos.

Artículo 123. *Creación.*

1. Los consorcios se crearán mediante convenio suscrito por las Administraciones, organismos públicos o entidades participantes.

2. En los consorcios en los que participe la Administración General del Estado o sus organismos públicos y entidades vinculados o dependientes se requerirá:

a) Que su creación se autorice por ley.

b) El convenio de creación precisará de autorización previa del Consejo de Ministros. La competencia para la suscripción del convenio no podrá ser objeto de delegación, y corresponderá al titular del departamento ministerial participante, y en el ámbito de los organismos autónomos, al titular del máximo órgano de dirección del organismo, previo informe del Ministerio del que dependa o al que esté vinculado.

c) Del convenio formarán parte los estatutos, un plan de actuación, de conformidad con lo previsto en el artículo 92, y una proyección presupuestaria trienal, además del informe preceptivo favorable del Ministerio de Hacienda y Administraciones Públicas. El convenio suscrito junto con los estatutos, así como sus modificaciones, serán objeto de publicación en el «Boletín Oficial del Estado».

Artículo 124. *Contenido de los estatutos.*

Los estatutos de cada consorcio determinarán la Administración Pública a la que estará adscrito, así como su régimen orgánico, funcional y financiero de acuerdo con lo previsto en esta Ley, y, al menos, los siguientes aspectos:

a) Sede, objeto, fines y funciones.

b) Identificación de participantes en el consorcio así como las aportaciones de sus miembros. A estos efectos, en aplicación del principio de responsabilidad previsto en el artículo 8 de la Ley Orgánica 2/2012, de 27 de abril, los estatutos incluirán cláusulas que limiten las actividades del consorcio si las entidades consorciadas incumplieran los compromisos de financiación o de cualquier otro tipo, así como fórmulas tendentes al aseguramiento de las cantidades comprometidas por las entidades consorciadas con carácter previo a la realización de las actividades presupuestadas.

c) Órganos de gobiernos y administración, así como su composición y funcionamiento, con indicación expresa del régimen de adopción de acuerdos. Podrán incluirse cláusulas que contemplen la suspensión temporal del derecho de voto o a la participación en la formación de los acuerdos cuando las Administraciones o entidades consorciadas incumplan manifiestamente sus obligaciones para con el consorcio, especialmente en lo que se refiere a los compromisos de financiación de las actividades del mismo.

d) Causas de disolución.

Artículo 125. *Causas y procedimiento para el ejercicio del derecho de separación de un consorcio.*

1. Los miembros de un consorcio, al que le resulte de aplicación lo previsto en esta Ley o en la Ley 7/1985, de 2 de abril, podrán separarse del mismo en cualquier momento siempre que no se haya señalado término para la duración del consorcio.

Cuando el consorcio tenga una duración determinada, cualquiera de sus miembros podrá separase antes de la finalización del plazo si alguno de los miembros del consorcio hubiera incumplido alguna de sus obligaciones estatutarias y, en particular, aquellas que impidan cumplir con el fin para el que fue creado el consorcio, como es la obligación de realizar aportaciones al fondo patrimonial.

Cuando un municipio deje de prestar un servicio, de acuerdo con lo previsto en la Ley 7/1985, de 2 de abril, y ese servicio sea uno de los prestados por el Consorcio al que pertenece, el municipio podrá separarse del mismo.

2. El derecho de separación habrá de ejercitarse mediante escrito notificado al máximo órgano de gobierno del consorcio. En el escrito deberá hacerse constar, en su caso, el incumplimiento que motiva la separación si el consorcio tuviera duración determinada, la formulación de requerimiento previo de su cumplimiento y el transcurso del plazo otorgado para cumplir tras el requerimiento.

Artículo 126. *Efectos del ejercicio del derecho de separación de un consorcio.*

1. El ejercicio del derecho de separación produce la disolución del consorcio salvo que el resto de sus miembros, de conformidad con lo previsto en sus estatutos, acuerden su continuidad y sigan permaneciendo en el consorcio, al menos, dos Administraciones, o entidades u organismos públicos vinculados o dependientes de más de una Administración.

2. Cuando el ejercicio del derecho de separación no conlleve la disolución del consorcio se aplicarán las siguientes reglas:

a) Se calculará la cuota de separación que corresponda a quien ejercite su derecho de separación, de acuerdo con la participación que le hubiera correspondido en el saldo resultante del patrimonio neto, de haber tenido lugar la liquidación, teniendo en cuenta el criterio de reparto dispuesto en los estatutos.

A falta de previsión estatutaria, se considerará cuota de separación la que le hubiera correspondido en la liquidación. En defecto de determinación de la cuota de liquidación se tendrán en cuenta, tanto el porcentaje de las aportaciones al fondo patrimonial del consorcio que haya efectuado quien ejerce el derecho de separación, como la financiación concedida cada año. Si el miembro del consorcio que se separa no hubiere realizado aportaciones por no estar obligado a ello, el criterio de reparto será la participación en los ingresos que, en su caso, hubiera recibido durante el tiempo que ha pertenecido al consorcio.

Se acordará por el consorcio la forma y condiciones en que tendrá lugar el pago de la cuota de separación, en el supuesto en que esta resulte positiva, así como la forma y condiciones del pago de la deuda que corresponda a quien ejerce el derecho de separación si la cuota es negativa.

La efectiva separación del consorcio se producirá una vez determinada la cuota de separación, en el supuesto en que ésta resulte positiva, o una vez se haya pagado la deuda, si la cuota es negativa.

b) Si el consorcio estuviera adscrito, de acuerdo con lo previsto en la Ley, a la Administración que ha ejercido el derecho de separación, tendrá que acordarse por el consorcio a quien se adscribe, de las restantes Administraciones o entidades u organismos públicos vinculados o dependientes de una Administración que permanecen en el consorcio, en aplicación de los criterios establecidos en la Ley.

Artículo 127. *Disolución del consorcio.*

1. La disolución del consorcio produce su liquidación y extinción. En todo caso será causa de disolución que los fines para los que fue creado el consorcio hayan sido cumplidos.

2. El máximo órgano de gobierno del consorcio al adoptar el acuerdo de disolución nombrará un liquidador que será un órgano o entidad, vinculada o dependiente, de la Administración Pública a la que el consorcio esté adscrito.

La responsabilidad que le corresponda al empleado público como miembro de la entidad u órgano liquidador será directamente asumida por la entidad o la Administración Pública que lo designó, quien podrá exigir de oficio al empleado público la responsabilidad que, en su caso, corresponda cuando haya concurrido dolo, culpa o negligencia graves conforme a lo previsto en las leyes administrativas en materia de responsabilidad patrimonial.

3. El liquidador calculará la cuota de liquidación que corresponda a cada miembro del consorcio de conformidad con lo previsto en los estatutos. Si no estuviera previsto en los estatutos, se calculará la mencionada cuota de acuerdo con la participación que le corresponda en el saldo resultante del patrimonio neto tras la liquidación, teniendo en cuenta que el criterio de reparto será el dispuesto en los estatutos.

A falta de previsión estatutaria, se tendrán en cuenta tanto el porcentaje de las aportaciones que haya efectuado cada miembro del consorcio al fondo patrimonial del mismo como la financiación concedida cada año. Si alguno de los miembros del consorcio no hubiere realizado aportaciones por no estar obligado a ello, el criterio de reparto será la participación en los ingresos que, en su caso, hubiera recibido durante el tiempo que ha pertenecido en el consorcio.

4. Se acordará por el consorcio la forma y condiciones en que tendrá lugar el pago de la cuota de liquidación en el supuesto en que ésta resulte positiva.

5. Las entidades consorciadas podrán acordar, con la mayoría que se establezca en los estatutos, o a falta de previsión estatutaria por unanimidad, la cesión global de activos y pasivos a otra entidad del sector público jurídicamente adecuada con la finalidad de mantener la continuidad de la actividad y alcanzar los objetivos del consorcio que se extingue. La cesión global de activos y pasivos implicará la extinción sin liquidación del consorcio cedente.

CAPÍTULO VII

De las fundaciones del sector público estatal

Artículo 128. *Definición y actividades propias.*

1. Son fundaciones del sector público estatal aquellas que reúnan alguno de los requisitos siguientes:

a) Que se constituyan de forma inicial, con una aportación mayoritaria, directa o indirecta, de la Administración General del Estado o cualquiera de los sujetos integrantes del sector público institucional estatal, o bien reciban dicha aportación con posterioridad a su constitución.

b) Que el patrimonio de la fundación esté integrado en más de un 50 por ciento por bienes o derechos aportados o cedidos por la Administración General del Estado o cualquiera de los sujetos integrantes del sector público institucional estatal con carácter permanente.

c) La mayoría de derechos de voto en su patronato corresponda a representantes de la Administración General del Estado o del sector público institucional estatal.

2. Son actividades propias de las fundaciones del sector público estatal las realizadas, sin ánimo de lucro, para el cumplimiento de fines de interés general, con independencia de que el servicio se preste de forma gratuita o mediante contraprestación.

Únicamente podrán realizar actividades relacionadas con el ámbito competencial de las entidades del sector público fundadoras, debiendo coadyuvar a la consecución de los fines de las mismas, sin que ello suponga la asunción de sus competencias propias, salvo previsión legal expresa. Las fundaciones no podrán ejercer potestades públicas.

En la denominación de las fundaciones del sector público estatal deberá figurar necesariamente la indicación «fundación del sector público» o su abreviatura «F.S.P.».

3. Para la financiación de las actividades y el mantenimiento de la fundación, debe haberse previsto la posibilidad de que en el patrimonio de las fundaciones del sector público pueda existir aportación del sector privado de forma no mayoritaria.

Artículo 129. *Régimen de adscripción de las fundaciones.*

1. Los estatutos de cada fundación determinarán la Administración Pública a la que estará adscrita de conformidad con lo previsto en este artículo.

2. De acuerdo con los siguientes criterios, ordenados por prioridad en su aplicación, referidos a la situación en el primer día del ejercicio presupuestario, la fundación del sector público quedará adscrita, en cada ejercicio presupuestario y por todo este periodo, a la Administración Pública que:

a) Disponga de mayoría de patronos.

b) Tenga facultades para nombrar o destituir a la mayoría de los miembros de los órganos ejecutivos.

c) Tenga facultades para nombrar o destituir a la mayoría de los miembros del personal directivo.

d) Tenga facultades para nombrar o destituir a la mayoría de los miembros del patronato.

e) Financie en más de un cincuenta por ciento, en su defecto, en mayor medida la actividad desarrollada por la fundación, teniendo en cuenta tanto la aportación del fondo patrimonial como la financiación concedida cada año.

f) Ostente el mayor porcentaje de participación en el fondo patrimonial.

g) Si la aplicación de los anteriores no resultara determinante, se adscribirá a la Administración General del Estado, y, en el caso de que ésta no participe, se adscribirá a la administración que decida su patronato.

3. En el supuesto de que participen en la fundación entidades privadas sin ánimo de lucro, la fundación del sector público estará adscrita a la Administración que resulte de acuerdo con los criterios establecidos en el apartado anterior.

4. El cambio de adscripción a una Administración Pública, cualquiera que fuere su causa, conllevará la modificación de los estatutos que deberá realizarse en un plazo no superior a tres meses, contados desde el inicio del ejercicio presupuestario siguiente a aquél en se produjo el cambio de adscripción.

5. Las fundaciones estarán sujetas al régimen presupuestario, económico financiero y de control de la Administración Pública a la que estén adscritas.

Artículo 130. *Régimen jurídico.*

Las fundaciones del sector público estatal se rigen por lo previsto en esta Ley, por la Ley 50/2002, de 26 de diciembre, de Fundaciones, la legislación autonómica que resulte aplicable en materia de fundaciones, y por el ordenamiento jurídico privado, salvo en las materias en que le sea de aplicación la normativa presupuestaria, contable, de control económico-financiero y de contratación del sector público.

Artículo 131. *Régimen de contratación.*

La contratación de las fundaciones del sector público estatal se ajustará a lo dispuesto en la legislación sobre contratación del sector público.

Artículo 132. *Régimen presupuestario, de contabilidad, de control económico-financiero y de personal.*

1. Las fundaciones del sector público estatal elaborarán anualmente un presupuesto de explotación y capital, que se integrarán con el Presupuesto General del Estado y formularán y presentarán sus cuentas de acuerdo con los principios y normas de contabilidad recogidos en la adaptación del Plan General de Contabilidad a las entidades sin fines lucrativos y disposiciones que lo desarrollan, así como la normativa vigente sobre fundaciones.

2. Las fundaciones del sector público estatal aplicarán el régimen presupuestario, económico financiero, de contabilidad, y de control establecido por la Ley 47/2003, de 26 de noviembre, y sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, estarán sometidas al control de la Intervención General de la Administración del Estado.

3. El personal de las fundaciones del sector público estatal, incluido el que tenga condición de directivo, se regirá por el Derecho laboral, así como por las normas que le sean de aplicación en función de su adscripción al sector público estatal, incluyendo entre las mismas la normativa presupuestaria así como lo que se establezca en las Leyes de Presupuestos Generales del Estado.

Artículo 133. *Creación de fundaciones del sector público estatal.*

1. La creación de las fundaciones del sector público estatal o la adquisición de este carácter de forma sobrevenida se realizará por ley que establecerá los fines de la fundación y, en su caso, los recursos económicos con los que se le dota.

2. El anteproyecto de ley de creación de una fundación del sector público estatal que se eleve al Consejo de Ministros deberá ser acompañado de una propuesta de estatutos y del plan de actuación, de conformidad con lo previsto en el artículo 92, junto con el informe

preceptivo favorable del Ministerio de Hacienda y Administraciones Públicas o la Intervención General de la Administración del Estado, según se determine reglamentariamente.

3. Los estatutos de las fundaciones del sector público estatal se aprobarán por Real Decreto de Consejo de Ministros, a propuesta conjunta del titular del Ministerio de Hacienda y Administraciones Públicas y del Ministerio que ejerza el protectorado, que estará determinado en sus Estatutos. No obstante, por Acuerdo del Consejo de Ministros podrá modificarse el Ministerio al que se adscriba inicialmente la fundación.

Artículo 134. *Protectorado.*

El Protectorado de las fundaciones del sector público será ejercido por el órgano de la Administración de adscripción que tenga atribuida tal competencia, que velará por el cumplimiento de las obligaciones establecidas en la normativa sobre fundaciones, sin perjuicio del control de eficacia y la supervisión continua al que están sometidas de acuerdo con lo previsto en esta Ley.

Artículo 135. *Estructura organizativa.*

En las fundaciones del sector público estatal la mayoría de miembros del patronato serán designados por los sujetos del sector público estatal.

La responsabilidad que le corresponda al empleado público como miembro del patronato será directamente asumida por la entidad o la Administración General del Estado que lo designó. La Administración General del Estado podrá exigir de oficio al empleado público que designó a esos efectos la responsabilidad en que hubiera incurrido por los daños y perjuicios causados en sus bienes o derechos cuando hubiera concurrido dolo, o culpa o negligencia graves, conforme a lo previsto en las leyes administrativas en materia de responsabilidad patrimonial.

Artículo 136. *Fusión, disolución, liquidación y extinción.*

A las fundaciones del sector público estatal le resultará de aplicación el régimen de fusión, disolución, liquidación y extinción previsto en los artículos 94, 96 y 97.

CAPÍTULO VIII

De los fondos carentes de personalidad jurídica del sector público estatal

Artículo 137. *Creación y extinción.*

1. La creación de fondos carentes de personalidad jurídica en el sector público estatal se efectuará por Ley. La norma de creación determinará expresamente su adscripción a la Administración General del Estado.

2. Con independencia de su creación por Ley se extinguirán por norma de rango reglamentario.

3. En la denominación de los fondos carentes de personalidad jurídica deberá figurar necesariamente la indicación «fondo carente de personalidad jurídica» o su abreviatura «F.C.P.J».

Artículo 138. *Régimen jurídico.*

Los fondos carentes de personalidad jurídica se regirán por lo dispuesto en esta Ley, en su norma de creación, y el resto de las normas de derecho administrativo general y especial que le sea de aplicación.

Artículo 139. *Régimen presupuestario, de contabilidad y de control económico-financiero.*

Los fondos carentes de personalidad jurídica estarán sujetos al régimen de presupuestación, contabilidad y control previsto en la Ley 47/2003, de 26 de noviembre.

TÍTULO III

Relaciones interadministrativas

CAPÍTULO I

Principios generales de las relaciones interadministrativas

Artículo 140. *Principios de las relaciones interadministrativas.*

1. Las diferentes Administraciones Públicas actúan y se relacionan con otras Administraciones y entidades u organismos vinculados o dependientes de éstas de acuerdo con los siguientes principios:

a) Lealtad institucional.
b) Adecuación al orden de distribución de competencias establecido en la Constitución y en los Estatutos de Autonomía y en la normativa del régimen local.
c) Colaboración, entendido como el deber de actuar con el resto de Administraciones Públicas para el logro de fines comunes.
d) Cooperación, cuando dos o más Administraciones Públicas, de manera voluntaria y en ejercicio de sus competencias, asumen compromisos específicos en aras de una acción común.
e) Coordinación, en virtud del cual una Administración Pública y, singularmente, la Administración General del Estado, tiene la obligación de garantizar la coherencia de las actuaciones de las diferentes Administraciones Públicas afectadas por una misma materia para la consecución de un resultado común, cuando así lo prevé la Constitución y el resto del ordenamiento jurídico.
f) Eficiencia en la gestión de los recursos públicos, compartiendo el uso de recursos comunes, salvo que no resulte posible o se justifique en términos de su mejor aprovechamiento.
g) Responsabilidad de cada Administración Pública en el cumplimiento de sus obligaciones y compromisos.
h) Garantía e igualdad en el ejercicio de los derechos de todos los ciudadanos en sus relaciones con las diferentes Administraciones.
i) Solidaridad interterritorial de acuerdo con la Constitución.

2. En lo no previsto en el presente Título, las relaciones entre la Administración General del Estado o las Administraciones de las Comunidades Autónomas con las Entidades que integran la Administración Local se regirán por la legislación básica en materia de régimen local.

CAPÍTULO II

Deber de colaboración

Artículo 141. *Deber de colaboración entre las Administraciones Públicas.*

1. Las Administraciones Públicas deberán:

a) Respetar el ejercicio legítimo por las otras Administraciones de sus competencias.
b) Ponderar, en el ejercicio de las competencias propias, la totalidad de los intereses públicos implicados y, en concreto, aquellos cuya gestión esté encomendada a las otras Administraciones.
c) Facilitar a las otras Administraciones la información que precisen sobre la actividad que desarrollen en el ejercicio de sus propias competencias o que sea necesaria para que los ciudadanos puedan acceder de forma integral a la información relativa a una materia.
d) Prestar, en el ámbito propio, la asistencia que las otras Administraciones pudieran solicitar para el eficaz ejercicio de sus competencias.
e) Cumplir con las obligaciones concretas derivadas del deber de colaboración y las restantes que se establezcan normativamente.

2. La asistencia y colaboración requerida sólo podrá negarse cuando el organismo público o la entidad del que se solicita no esté facultado para prestarla de acuerdo con lo previsto en su normativa específica, no disponga de medios suficientes para ello o cuando, de hacerlo, causara un perjuicio grave a los intereses cuya tutela tiene encomendada o al cumplimiento de sus propias funciones o cuando la información solicitada tenga carácter confidencial o reservado. La negativa a prestar la asistencia se comunicará motivadamente a la Administración solicitante.

3. La Administración General del Estado, las de las Comunidades Autónomas y las de las Entidades Locales deberán colaborar y auxiliarse para la ejecución de sus actos que hayan de realizarse o tengan efectos fuera de sus respectivos ámbitos territoriales. Los posibles costes que pueda generar el deber de colaboración podrán ser repercutidos cuando así se acuerde.

Artículo 142. *Técnicas de colaboración.*

Las obligaciones que se derivan del deber de colaboración se harán efectivas a través de las siguientes técnicas:

a) El suministro de información, datos, documentos o medios probatorios que se hallen a disposición del organismo público o la entidad al que se dirige la solicitud y que la Administración solicitante precise disponer para el ejercicio de sus competencias.

b) La colaboración a fin de proporcionar la inclusión en un sistema integrado de información de las respectivas áreas personalizadas o carpetas ciudadanas, o determinadas funcionalidades de las mismas, de forma que el interesado pueda acceder a sus contenidos, notificaciones o funcionalidades mediante procedimientos seguros que garanticen la integridad y confidencialidad de los datos de carácter personal, independientemente de cuál haya sido el punto de acceso.

c) El desarrollo de la Plataforma Digital de Colaboración entre las Administraciones Públicas como instrumento destinado a facilitar las relaciones y el soporte electrónico de los órganos integrantes del sistema de Conferencias Sectoriales y en general de los órganos de cooperación, así como de otras de plataformas comunes para el intercambio de datos en el ámbito de todas las administraciones públicas.

d) La creación y mantenimiento de sistemas integrados de información administrativa con el fin de disponer de datos actualizados, completos y permanentes referentes a los diferentes ámbitos de actividad administrativa en todo el territorio nacional.

e) El deber de asistencia y auxilio, para atender las solicitudes formuladas por otras Administraciones para el mejor ejercicio de sus competencias, en especial cuando los efectos de su actividad administrativa se extiendan fuera de su ámbito territorial.

f) Cualquier otra prevista en una Ley.

CAPÍTULO III

Relaciones de cooperación

Sección 1.ª Técnicas de cooperación

Artículo 143. *Cooperación entre Administraciones Públicas.*

1. Las Administraciones cooperarán al servicio del interés general y podrán acordar de manera voluntaria la forma de ejercer sus respectivas competencias que mejor sirva a este principio.

2. La formalización de relaciones de cooperación requerirá la aceptación expresa de las partes, formulada en acuerdos de órganos de cooperación o en convenios.

Artículo 144. *Técnicas de Cooperación.*

1. Se podrá dar cumplimiento al principio de cooperación de acuerdo con las técnicas que las Administraciones interesadas estimen más adecuadas, como pueden ser:

a) La participación en órganos de cooperación, con el fin de deliberar y, en su caso, acordar medidas en materias sobre las que tengan competencias diferentes Administraciones Públicas.

b) La participación en órganos consultivos de otras Administraciones Públicas.

c) La participación de una Administración Pública en organismos públicos o entidades dependientes o vinculados a otra Administración diferente.

d) La prestación de medios materiales, económicos o personales a otras Administraciones Públicas.

e) La cooperación interadministrativa para la aplicación coordinada de la normativa reguladora de una determinada materia.

f) La emisión de informes no preceptivos con el fin de que las diferentes Administraciones expresen su criterio sobre propuestas o actuaciones que incidan en sus competencias.

g) Las actuaciones de cooperación en materia patrimonial, incluidos los cambios de titularidad y la cesión de bienes, previstas en la legislación patrimonial.

h) Cualquier otra prevista en la Ley.

2. En los convenios y acuerdos en los que se formalice la cooperación se preverán las condiciones y compromisos que asumen las partes que los suscriben.

3. Cada Administración Pública mantendrá actualizado un registro electrónico de los órganos de cooperación en los que participe y de convenios que haya suscrito.

Sección 2.ª Técnicas orgánicas de cooperación

Artículo 145. *Órganos de cooperación.*

1. Los órganos de cooperación son órganos de composición multilateral o bilateral, de ámbito general o especial, constituidos por representantes de la Administración General del Estado, de las Administraciones de las Comunidades o Ciudades de Ceuta y Melilla o, en su caso, de las Entidades Locales, para acordar voluntariamente actuaciones que mejoren el ejercicio de las competencias que cada Administración Pública tiene.

2. Los órganos de cooperación se regirán por lo dispuesto en esta Ley y por las disposiciones específicas que les sean de aplicación.

3. Los órganos de cooperación entre distintas Administraciones Públicas en los que participe la Administración General del Estado, deberán inscribirse en el Registro estatal de Órganos e Instrumentos de Cooperación para que resulte válida su sesión constitutiva.

4. Los órganos de cooperación, salvo oposición por alguna de las partes, podrán adoptar acuerdos a través de un procedimiento simplificado y por suscripción sucesiva de las partes, por cualquiera de las formas admitidas en Derecho, en los términos que se establezcan de común acuerdo.

Artículo 146. *Conferencia de Presidentes.*

1. La Conferencia de Presidentes es un órgano de cooperación multilateral entre el Gobierno de la Nación y los respectivos Gobiernos de las Comunidades Autónomas y está formada por el Presidente del Gobierno, que la preside, y por los Presidentes de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla.

2. La Conferencia de Presidentes tiene por objeto la deliberación de asuntos y la adopción de acuerdos de interés para el Estado y las Comunidades Autónomas, estando asistida para la preparación de sus reuniones por un Comité preparatorio del que forman parte un Ministro del Gobierno, que lo preside, y un Consejero de cada Comunidad Autónoma.

Artículo 147. *Conferencias Sectoriales.*

1. La Conferencia Sectorial es un órgano de cooperación, de composición multilateral y ámbito sectorial determinado, que reúne, como Presidente, al miembro del Gobierno que, en representación de la Administración General del Estado, resulte competente por razón de la materia, y a los correspondientes miembros de los Consejos de Gobierno, en representación de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla.

2. Las Conferencias Sectoriales, u órganos sometidos a su régimen jurídico con otra denominación, habrán de inscribirse en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación para su válida constitución.

3. Cada Conferencia Sectorial dispondrá de un reglamento de organización y funcionamiento interno aprobado por sus miembros.

Artículo 148. *Funciones de las Conferencias Sectoriales.*

1. Las Conferencias Sectoriales pueden ejercer funciones consultivas, decisorias o de coordinación orientadas a alcanzar acuerdos sobre materias comunes.

2. En particular, las Conferencias Sectoriales ejercerán, entre otras, las siguientes funciones:

a) Ser informadas sobre los anteproyectos de leyes y los proyectos de reglamentos del Gobierno de la Nación o de los Consejos de Gobierno de las Comunidades Autónomas cuando afecten de manera directa al ámbito competencial de las otras Administraciones Públicas o cuando así esté previsto en la normativa sectorial aplicable, bien a través de su pleno o bien a través de la comisión o el grupo de trabajo mandatado al efecto.

b) Establecer planes específicos de cooperación entre Comunidades Autónomas en la materia sectorial correspondiente, procurando la supresión de duplicidades, y la consecución de una mejor eficiencia de los servicios públicos.

c) Intercambiar información sobre las actuaciones programadas por las distintas Administraciones Públicas, en ejercicio de sus competencias, y que puedan afectar a las otras Administraciones.

d) Establecer mecanismos de intercambio de información, especialmente de contenido estadístico.

e) Acordar la organización interna de la Conferencia Sectorial y de su método de trabajo.

f) Fijar los criterios objetivos que sirvan de base para la distribución territorial de los créditos presupuestarios, así como su distribución al comienzo del ejercicio económico, de acuerdo con lo previsto en la Ley 47/2003, de 26 de noviembre.

Artículo 149. *Convocatoria de las reuniones de las Conferencias Sectoriales.*

1. Corresponde al Ministro que presida la Conferencia Sectorial acordar la convocatoria de las reuniones por iniciativa propia, al menos una vez al año, o cuando lo soliciten, al menos, la tercera parte de sus miembros. En este último caso, la solicitud deberá incluir la propuesta de orden del día.

2. La convocatoria, que deberá acompañarse de los documentos necesarios con la suficiente antelación, deberá contener el orden del día previsto para cada sesión, sin que puedan examinarse asuntos que no figuren en el mismo, salvo que todos los miembros de la Conferencia Sectorial manifiesten su conformidad. El orden del día de cada reunión será propuesto por el Presidente y deberá especificar el carácter consultivo, decisorio o de coordinación de cada uno de los asuntos a tratar.

3. Cuando la conferencia sectorial hubiera de reunirse con el objeto exclusivo de informar un proyecto normativo, la convocatoria, la constitución y adopción de acuerdos podrá efectuarse por medios electrónicos, telefónicos o audiovisuales, que garanticen la intercomunicación entre ellos y la unidad de acto, tales como la videoconferencia o el correo electrónico, entendiéndose los acuerdos adoptados en el lugar donde esté la presidencia, de acuerdo con el procedimiento que se establezca en el reglamento de funcionamiento interno de la conferencia sectorial.

De conformidad con lo previsto en este apartado la elaboración y remisión de actas podrá realizarse a través de medios electrónicos.

Artículo 150. *Secretaría de las Conferencias Sectoriales.*

1. Cada Conferencia Sectorial tendrá un secretario que será designado por el Presidente de la Conferencia Sectorial.

2. Corresponde al secretario de la Conferencia Sectorial, al menos, las siguientes funciones:

a) Preparar las reuniones y asistir a ellas con voz pero sin voto.

b) Efectuar la convocatoria de las sesiones de la Conferencia Sectorial por orden del Presidente.

c) Recibir los actos de comunicación de los miembros de la Conferencia Sectorial y, por tanto, las notificaciones, peticiones de datos, rectificaciones o cualquiera otra clase de escritos de los que deba tener conocimiento.

d) Redactar y autorizar las actas de las sesiones.

e) Expedir certificaciones de las consultas, recomendaciones y acuerdos aprobados y custodiar la documentación generada con motivo de la celebración de sus reuniones.

f) Cuantas otras funciones sean inherentes a su condición de secretario.

Artículo 151. *Clases de decisiones de la Conferencia Sectorial.*

1. La adopción de decisiones requerirá la previa votación de los miembros de la Conferencia Sectorial. Esta votación se producirá por la representación que cada Administración Pública tenga y no por los distintos miembros de cada una de ellas.

2. Las decisiones que adopte la Conferencia Sectorial podrán revestir la forma de:

a) Acuerdo: supone un compromiso de actuación en el ejercicio de las respectivas competencias. Son de obligado cumplimiento y directamente exigibles de acuerdo con lo previsto en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, salvo para quienes hayan votado en contra mientras no decidan suscribirlos con posterioridad. El acuerdo será certificado en acta.

Cuando la Administración General del Estado ejerza funciones de coordinación, de acuerdo con el orden constitucional de distribución de competencias del ámbito material respectivo, el Acuerdo que se adopte en la Conferencia Sectorial, y en el que se incluirán los votos particulares que se hayan formulado, será de obligado cumplimiento para todas las Administraciones Públicas integrantes de la Conferencia Sectorial, con independencia del sentido de su voto, siendo exigibles conforme a lo establecido en la Ley 29/1998, de 13 de julio. El acuerdo será certificado en acta.

Las Conferencias Sectoriales podrán adoptar planes conjuntos, de carácter multilateral, entre la Administración General del Estado y la de las Comunidades Autónomas, para comprometer actuaciones conjuntas para la consecución de los objetivos comunes, que tendrán la naturaleza de Acuerdo de la conferencia sectorial y se publicarán en el «Boletín Oficial del Estado».

El acuerdo aprobatorio de los planes deberá especificar, según su naturaleza, los siguientes elementos, de acuerdo con lo previsto en la legislación presupuestaria:

1.º Los objetivos de interés común a cumplir.
2.º Las actuaciones a desarrollar por cada Administración.
3.º Las aportaciones de medios personales y materiales de cada Administración.
4.º Los compromisos de aportación de recursos financieros.
5.º La duración, así como los mecanismos de seguimiento, evaluación y modificación.

b) Recomendación: tiene como finalidad expresar la opinión de la Conferencia Sectorial sobre un asunto que se somete a su consulta. Los miembros de la Conferencia Sectorial se comprometen a orientar su actuación en esa materia de conformidad con lo previsto en la Recomendación salvo quienes hayan votado en contra mientras no decidan suscribirla con posterioridad. Si algún miembro se aparta de la Recomendación, deberá motivarlo e incorporar dicha justificación en el correspondiente expediente.

Artículo 152. *Comisiones Sectoriales y Grupos de trabajo.*

1. La Comisión Sectorial es el órgano de trabajo y apoyo de carácter general de la Conferencia Sectorial, estando constituida por el Secretario de Estado u órgano superior de la Administración General del Estado designado al efecto por el Ministro correspondiente, que la presidirá, y un representante de cada Comunidad Autónoma, así como un representante de la Ciudad de Ceuta y de la Ciudad Melilla. El ejercicio de las funciones propias de la secretaría de la Comisión Sectorial corresponderá a un funcionario del Ministerio correspondiente.

Si así se prevé en el reglamento interno de funcionamiento de la Conferencia Sectorial, las comisiones sectoriales y grupos de trabajo podrán funcionar de forma electrónica o por medios telefónicos o audiovisuales, que garanticen la intercomunicación entre ellos y la unidad de acto, tales como la videoconferencia o el correo electrónico, entendiendo los acuerdos adoptados en el lugar donde esté la presidencia, de acuerdo con el procedimiento que se establezca en el reglamento de funcionamiento interno de la Conferencia Sectorial.

2. La Comisión Sectorial ejercerá las siguientes funciones:

a) La preparación de las reuniones de la Conferencia Sectorial, para lo que tratará los asuntos incluidos en el orden del día de la convocatoria.

b) El seguimiento de los acuerdos adoptados por la Conferencia Sectorial.

c) El seguimiento y evaluación de los Grupos de trabajo constituidos.

d) Cualquier otra que le encomiende la Conferencia Sectorial.

3. Las Conferencias Sectoriales podrán crear Grupos de trabajo, de carácter permanente o temporal, formados por Directores Generales, Subdirectores Generales o equivalentes de las diferentes Administraciones Públicas que formen parte de dicha Conferencia, para llevar a cabo las tareas técnicas que les asigne la Conferencia Sectorial o la Comisión Sectorial. A estos grupos de trabajo podrán ser invitados expertos de reconocido prestigio en la materia a tratar.

El director del Grupo de trabajo, que será un representante de la Administración General del Estado, podrá solicitar con el voto favorable de la mayoría de sus miembros, la participación en el mismo de las organizaciones representativas de intereses afectados, con el fin de recabar propuestas o formular consultas.

Artículo 153. *Comisiones Bilaterales de Cooperación.*

1. Las Comisiones Bilaterales de Cooperación son órganos de cooperación de composición bilateral que reúnen, por un número igual de representantes, a miembros del Gobierno, en representación de la Administración General del Estado, y miembros del Consejo de Gobierno de la Comunidad Autónoma o representantes de la Ciudad de Ceuta o de la Ciudad de Melilla.

2. Las Comisiones Bilaterales de Cooperación ejercen funciones de consulta y adopción de acuerdos que tengan por objeto la mejora de la coordinación entre las respectivas Administraciones en asuntos que afecten de forma singular a la Comunidad Autónoma, a la Ciudad de Ceuta o a la Ciudad de Melilla.

3. Para el desarrollo de su actividad, las Comisiones Bilaterales de Cooperación podrán crear Grupos de trabajo y podrán convocarse y adoptar acuerdos por videoconferencia o por medios electrónicos.

4. Las decisiones adoptadas por las Comisiones Bilaterales de Cooperación revestirán la forma de Acuerdos y serán de obligado cumplimiento, cuando así se prevea expresamente, para las dos Administraciones que lo suscriban y en ese caso serán exigibles conforme a lo establecido en la Ley 29/1998, de 13 de julio. El acuerdo será certificado en acta.

5. Lo previsto en este artículo será de aplicación sin perjuicio de las peculiaridades que, de acuerdo con las finalidades básicas previstas, se establezcan en los Estatutos de Autonomía en materia de organización y funciones de las comisiones bilaterales.

Artículo 154. *Comisiones Territoriales de Coordinación.*

1. Cuando la proximidad territorial o la concurrencia de funciones administrativas así lo requiera, podrán crearse Comisiones Territoriales de Coordinación, de composición multilateral, entre Administraciones cuyos territorios sean coincidentes o limítrofes, para mejorar la coordinación de la prestación de servicios, prevenir duplicidades y mejorar la eficiencia y calidad de los servicios. En función de las Administraciones afectadas por razón de la materia, estas Comisiones podrán estar formadas por:

a) Representantes de la Administración General del Estado y representantes de las Entidades Locales.

b) Representantes de las Comunidades Autónomas y representantes de las Entidades locales.

c) Representantes de la Administración General del Estado, representantes de las Comunidades Autónomas y representantes de las Entidades Locales.

2. La decisiones adoptadas por las Comisiones Territoriales de Cooperación revestirán la forma de Acuerdos, que serán certificados en acta y serán de obligado cumplimiento para las Administraciones que lo suscriban y exigibles conforme a lo establecido en la Ley 29/1998, de 13 de julio.

3. El régimen de las convocatorias y la secretaría será el mismo que el establecido para las Conferencias Sectoriales en los artículos 149 y 150, salvo la regla prevista sobre quién debe ejercer las funciones de secretario, que se designará según su reglamento interno de funcionamiento.

CAPÍTULO IV

Relaciones electrónicas entre las Administraciones

Artículo 155. *Transmisiones de datos entre Administraciones Públicas.*

1. De conformidad con lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de seguridad, integridad y disponibilidad.

2. En ningún caso podrá procederse a un tratamiento ulterior de los datos para fines incompatibles con el fin para el cual se recogieron inicialmente los datos personales. De acuerdo con lo previsto en el artículo 5.1.b) del Reglamento (UE) 2016/679, no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.

3. Fuera del caso previsto en el apartado anterior y siempre que las leyes especiales aplicables a los respectivos tratamientos no prohíban expresamente el tratamiento ulterior de los datos para una finalidad distinta, cuando la Administración Pública cesionaria de los datos pretenda el tratamiento ulterior de los mismos para una finalidad que estime compatible con el fin inicial, deberá comunicarlo previamente a la Administración Pública cedente a los efectos de que esta pueda comprobar dicha compatibilidad. La Administración Pública cedente podrá, en el plazo de diez días oponerse motivadamente. Cuando la Administración cedente sea la Administración General del Estado podrá en este supuesto, excepcionalmente y de forma motivada, suspender la transmisión de datos por razones de seguridad nacional de forma cautelar por el tiempo estrictamente indispensable para su preservación. En tanto que la Administración Pública cedente no comunique su decisión a la cesionaria esta no podrá emplear los datos para la nueva finalidad pretendida.

Se exceptúan de lo dispuesto en el párrafo anterior los supuestos en que el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales esté previsto en una norma con rango de ley de conformidad con lo previsto en el artículo 23.1 del Reglamento (UE) 2016/679.

Artículo 156. *Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.*

1. El Esquema Nacional de Interoperabilidad comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido

por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Artículo 157. *Reutilización de sistemas y aplicaciones de propiedad de la Administración.*

1. Las Administraciones pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información.

3. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el directorio general de aplicaciones, dependiente de la Administración General del Estado, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

En este directorio constarán tanto las aplicaciones disponibles de la Administración General del Estado como las disponibles en los directorios integrados de aplicaciones del resto de Administraciones.

En el caso de existir una solución disponible para su reutilización total o parcial, las Administraciones Públicas estarán obligadas a su uso, salvo que la decisión de no reutilizarla se justifique en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Artículo 158. *Transferencia de tecnología entre Administraciones.*

1. Las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad. Estos directorios deberán ser plenamente interoperables con el directorio general de la Administración General del Estado, de modo que se garantice su compatibilidad informática e interconexión.

2. La Administración General del Estado, mantendrá un directorio general de aplicaciones para su reutilización, prestará apoyo para la libre reutilización de aplicaciones e impulsará el desarrollo de aplicaciones, formatos y estándares comunes en el marco de los esquemas nacionales de interoperabilidad y seguridad.

Disposición adicional primera. *Administración de los Territorios Históricos del País Vasco.*

En la Comunidad Autónoma del País Vasco, a efectos de lo dispuesto en el artículo segundo, se entenderá por Administraciones Públicas las Diputaciones Forales y las Administraciones institucionales de ellas dependientes o vinculadas.

Disposición adicional segunda. *Delegados del Gobierno en las Ciudades de Ceuta y Melilla.*

1. En las Ciudades de Ceuta y Melilla existirá un Delegado del Gobierno que representará al Gobierno de la Nación en su territorio.

2. Las disposiciones contenidas en la presente Ley que hagan referencia a los Delegados del Gobierno en las Comunidades Autónomas se deberán entender también referidas a los Delegados del Gobierno en las Ciudades de Ceuta y Melilla.

3. En las Ciudades de Ceuta y Melilla existirá una Comisión de asistencia al Delegado del Gobierno, presidida por él mismo e integrada por el Secretario General y los responsables de los servicios territoriales. A sus sesiones deberán asistir los titulares de los

órganos y servicios territoriales, tanto integrados como no integrados que el Delegado del Gobierno considere oportuno.

Disposición adicional tercera. *Relaciones con las ciudades de Ceuta y Melilla.*

Lo dispuesto en esta Ley sobre las relaciones entre la Administración General del Estado y las Administraciones de las Comunidades Autónomas será de aplicación a las relaciones con las Ciudades de Ceuta y Melilla en la medida en que afecte al ejercicio de las competencias estatutariamente asumidas.

Disposición adicional cuarta. *Adaptación de entidades y organismos públicos existentes en el ámbito estatal.*

Las entidades con régimen jurídico específico a la entrada en vigor de esta ley se seguirán rigiendo por su legislación específica, manteniendo su naturaleza jurídica, y únicamente de forma supletoria, y en tanto resulte compatible con su legislación específica por lo previsto en esta ley.

Los demás organismos y entidades, a los que se refiere el artículo 84.1 de esta ley, existentes en el momento de la entrada en vigor de la misma, deberán adaptarse a su contenido antes del 1 de octubre de 2024, rigiéndose hasta que se realice la adaptación por su normativa específica.

La adaptación se realizará preservando las actuales especialidades de los organismos y entidades en materia de personal, patrimonio, régimen presupuestario, contabilidad, control económico-financiero y de operaciones como agente de financiación, incluyendo, respecto a estas últimas, el sometimiento, en su caso, al ordenamiento jurídico privado. Las especialidades se preservarán siempre que no hubieran generado deficiencias importantes en el control de ingresos y gastos causantes de una situación de desequilibrio financiero en el momento de su adaptación.

Las entidades que no tuvieran la consideración de poder adjudicador, preservarán esta especialidad en tanto no se oponga a la normativa comunitaria.

Disposición adicional quinta. *Gestión compartida de servicios comunes de los organismos públicos estatales existentes.*

1. Los organismos públicos integrantes del sector público estatal a la entrada en vigor de esta ley compartirán la organización y gestión de sus servicios comunes salvo que la decisión de no compartirlos se justifique, en una memoria elaborada al efecto y que se dirigirá al Ministerio de Hacienda y Administraciones Públicas, en términos de eficiencia, conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, en razones de seguridad nacional, o cuando la organización y gestión compartida afecte a servicios que deban prestarse de forma autónoma en atención a la independencia del organismo público.

2. La organización y gestión compartida de los servicios comunes a los que se refiere el artículo 95 podrá realizarse de las formas siguientes:

a) Mediante su coordinación por el departamento con competencias en materia de Hacienda pública o por un organismo autónomo vinculado o dependiente del mismo.

b) Mediante su coordinación por el departamento al que esté vinculado o del que dependa el organismo público.

c) Mediante su coordinación por el organismo público al que esté vinculado o del que dependa a su vez el organismo público.

Disposición adicional sexta. *Transformación de los medios propios estatales existentes.*

Todas las entidades y organismos públicos que en el momento de la entrada en vigor de esta Ley tengan la condición de medio propio en el ámbito estatal deberán adaptarse a lo previsto en esta Ley en el plazo de seis meses a contar desde su entrada en vigor.

Disposición adicional séptima. *Registro Electrónico estatal de Órganos e Instrumentos de Cooperación.*

1. La Administración General del Estado mantendrá actualizado un registro electrónico de los órganos de cooperación en los que participa ella o alguno de sus organismos públicos o entidades vinculados o dependientes y de convenios celebrados con el resto de Administraciones Públicas. Este registro será dependiente de la Secretaría de Estado de Administraciones Públicas.

2. La creación, modificación o extinción de los órganos de cooperación, así como la suscripción, extinción, prórroga o modificación de cualquier convenio celebrado por la Administración General del Estado o alguno de sus organismos públicos o entidades vinculados o dependientes deberá ser comunicada por el órgano de ésta que lo haya suscrito, en el plazo de cinco días desde que ocurra el hecho inscribible, al Registro Electrónico estatal de Órganos e Instrumentos de Cooperación.

3. Los Departamentos Ministeriales que ejerzan la Secretaría de los órganos de cooperación deberán comunicar al registro antes del 30 de enero de cada año los órganos de cooperación que hayan extinguido.

4. El Ministro de Hacienda y Administraciones Públicas elevará anualmente al Consejo de Ministros un informe sobre la actividad de los órganos de cooperación existentes, así como sobre los convenios vigentes a partir de los datos y análisis proporcionados por el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación.

5. Los órganos de cooperación y los convenios vigentes disponen del plazo de seis meses, a contar desde la entrada en vigor de la Ley, para solicitar su inscripción en este Registro.

6. Los órganos de cooperación que no se hayan reunido en un plazo de cinco años desde su creación o en un plazo de cinco años desde la entrada en vigor de esta ley quedarán extinguidos.

Disposición adicional octava. *Adaptación de los convenios vigentes suscritos por cualquier Administración Pública e inscripción de organismos y entidades en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local.*

1. Todos los convenios vigentes suscritos por cualquier Administración Pública o cualquiera de sus organismos o entidades vinculados o dependientes deberán adaptarse a lo aquí previsto en el plazo de tres años a contar desde la entrada en vigor de esta Ley.

No obstante, esta adaptación será automática, en lo que se refiere al plazo de vigencia del convenio, por aplicación directa de las reglas previstas en el artículo 49.h).1.º para los convenios que no tuvieran determinado un plazo de vigencia o, existiendo, tuvieran establecida una prórroga tácita por tiempo indefinido en el momento de la entrada en vigor de esta Ley. En estos casos el plazo de vigencia del convenio será de cuatro años a contar desde la entrada en vigor de la presente Ley.

2. Todos los organismos y entidades, vinculados o dependientes de cualquier Administración Pública y cualquiera que sea su naturaleza jurídica, existentes en el momento de la entrada en vigor de esta Ley deberán estar inscritos en el Inventario de Entidades del Sector Público Estatal, Autonómico y Local en el plazo de tres meses a contar desde dicha entrada en vigor.

Disposición adicional novena. *Comisión Sectorial de administración electrónica.*

1. La Comisión Sectorial de administración electrónica, dependiente de la Conferencia Sectorial de Administración Pública, es el órgano técnico de cooperación de la Administración General del Estado, de las Administraciones de las Comunidades Autónomas y de las Entidades Locales en materia de administración electrónica.

2. La Comisión Sectorial de la administración electrónica desarrollará, al menos, las siguientes funciones:

a) Asegurar la compatibilidad e interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones Públicas.

b) Impulsar el desarrollo de la administración electrónica en España.

c) Asegurar la cooperación entre las Administraciones Públicas para proporcionar información administrativa clara, actualizada e inequívoca.

3. Cuando por razón de las materias tratadas resulte de interés, podrá invitarse a las organizaciones, corporaciones o agentes sociales que se estime conveniente en cada caso a participar en las deliberaciones de la Comisión Sectorial.

Disposición adicional décima. *Aportaciones a los consorcios.*

Cuando las Administraciones Públicas o cualquiera de sus organismos públicos o entidades vinculados o dependientes sean miembros de un consorcio, no estarán obligados a efectuar la aportación al fondo patrimonial o la financiación a la que se hayan comprometido para el ejercicio corriente si alguno de los demás miembros del consorcio no hubiera realizado la totalidad de sus aportaciones dinerarias correspondientes a ejercicios anteriores a las que estén obligados.

Disposición adicional undécima. *Conflictos de atribuciones intraministeriales.*

1. Los conflictos positivos o negativos de atribuciones entre órganos de un mismo Ministerio serán resueltos por el superior jerárquico común en el plazo de diez días, sin que quepa recurso alguno.

2. En los conflictos positivos, el órgano que se considere competente requerirá de inhibición al que conozca del asunto, quien suspenderá el procedimiento por un plazo de diez días. Si dentro de dicho plazo acepta el requerimiento, remitirá el expediente al órgano requirente. En caso de considerarse competente, remitirá acto seguido las actuaciones al superior jerárquico común.

3. En los conflictos negativos, el órgano que se estime incompetente remitirá directamente las actuaciones al órgano que considere competente, quien decidirá en el plazo de diez días y, en su caso, de considerarse, asimismo, incompetente, remitirá acto seguido el expediente con su informe al superior jerárquico común.

4. Los interesados en el procedimiento plantearán estos conflictos de acuerdo a lo establecido en el artículo 14.

Disposición adicional duodécima. *Régimen Jurídico de las Autoridades Portuarias y Puertos del Estado.*

Las Autoridades Portuarias y Puertos del Estado se regirán por su legislación específica, por las disposiciones de la Ley 47/2003, de 26 de noviembre, que les sean de aplicación y, supletoriamente, por lo establecido en esta Ley.

Disposición adicional decimotercera. *Régimen jurídico de las Entidades gestoras y servicios comunes de la Seguridad Social.*

1. A las Entidades gestoras, servicios comunes y otros organismos o entidades que conforme a la Ley integran la Administración de la Seguridad Social, les será de aplicación las previsiones de esta Ley relativas a los organismos autónomos, salvo lo dispuesto en el párrafo siguiente.

2. El régimen de personal, económico-financiero, patrimonial, presupuestario y contable, de participación en la gestión, así como la asistencia jurídica, será el establecido por su legislación específica, por la Ley 47/2003, de 26 de noviembre, General Presupuestaria, en las materias que sea de aplicación, y supletoriamente por esta Ley.

Disposición adicional decimocuarta. *La organización militar y las Delegaciones de Defensa.*

1. La organización militar se rige por su legislación específica y por las bases establecidas en la ley Orgánica 5/2005, de 17 de noviembre, de la Defensa Nacional.

2. Las Delegaciones de Defensa permanecerán integradas en el Ministerio de Defensa y se regirán por su normativa específica.

Disposición adicional decimoquinta. *Personal militar de las Fuerzas Armadas y del Centro Nacional de Inteligencia.*

Las referencias que en los artículos 63, 65, 66 y 67 de esta ley se realizan a los funcionarios de carrera pertenecientes al Subgrupo A1 comprenderán al personal militar de las Fuerzas Armadas perteneciente a cuerpos y escalas con una categoría equivalente a aquélla.

Dichas previsiones normativas serán igualmente aplicables al personal del Centro Nacional de Inteligencia perteneciente al Subgrupo A1, según su normativa estatutaria.

Disposición adicional decimosexta. *Servicios territoriales integrados en las Delegaciones del Gobierno.*

Los servicios territoriales que, a la entrada en vigor de esta Ley, estuviesen integrados en las Delegaciones del Gobierno continuarán en esta situación, siendo aplicable a los mismos lo previsto en la presente Ley.

Disposición adicional decimoséptima. *Régimen jurídico de la Agencia Estatal de Administración Tributaria.*

La Agencia Estatal de Administración Tributaria se regirá por su legislación específica y únicamente de forma supletoria y en tanto resulte compatible con su legislación específica por lo previsto en esta Ley.

El acceso, la cesión o la comunicación de información de naturaleza tributaria se regirán en todo caso por su legislación específica.

Disposición adicional decimoctava. *Régimen jurídico del Centro Nacional de Inteligencia.*

La actuación administrativa de los órganos competentes del Centro Nacional de Inteligencia se regirá por lo previsto en su normativa específica y en lo no previsto en ella, en cuanto sea compatible con su naturaleza y funciones propias, por lo dispuesto en la presente Ley.

Disposición adicional decimonovena. *Régimen jurídico del Banco de España.*

El Banco de España en su condición de banco central nacional se regirá, en primer término, por lo dispuesto en el Tratado de Funcionamiento de la Unión Europea, los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo, el Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013 y la Ley 13/1994, de 1 de junio, de Autonomía del Banco de España.

En lo no previsto en las referidas normas y en cuanto sea compatible con su naturaleza y funciones será de aplicación lo previsto en la presente Ley.

Disposición adicional vigésima. *Régimen jurídico del Fondo de Reestructuración Ordenada Bancaria.*

El Fondo de Reestructuración Ordenada Bancaria tendrá la consideración de autoridad administrativa independiente de conformidad con lo previsto en esta Ley.

Disposición adicional vigesimoprimera. *Órganos Colegiados de Gobierno.*

Las disposiciones previstas en esta Ley relativas a los órganos colegiados no serán de aplicación a los órganos Colegiados del Gobierno de la Nación, los órganos colegiados de Gobierno de las Comunidades Autónomas y los órganos colegiados de gobierno de las Entidades Locales.

Disposición adicional vigesimosegunda. *Actuación administrativa de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos.*

La actuación administrativa de los órganos competentes del Congreso de los Diputados, del Senado, del Consejo General del Poder Judicial, del Tribunal Constitucional, del Tribunal de Cuentas, del Defensor del Pueblo, de las Asambleas Legislativas de las Comunidades

Autónomas y de las instituciones autonómicas análogas al Tribunal de Cuentas y al Defensor del Pueblo, se regirá por lo previsto en su normativa específica, en el marco de los principios que inspiran la actuación administrativa de acuerdo con esta Ley.

Disposición adicional vigesimotercera. *Régimen jurídico aplicable a la entidad pública empresarial Sociedad de Salvamento y Seguridad Marítima.*

La Sociedad de Salvamento y Seguridad Marítima (SASEMAR) preservará su naturaleza de entidad pública empresarial y, con las especialidades contenidas en su legislación específica, se regirá por las disposiciones aplicables a dichas entidades en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a excepción de lo dispuesto en los artículos 103.1 y 107.3 de la Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional vigesimocuarta. *Régimen jurídico aplicable a la entidad pública empresarial Centro para el Desarrollo Tecnológico e Industrial.*

El Centro para el Desarrollo Tecnológico e Industrial (CDTI) preservará su naturaleza de entidad pública empresarial y, con las especialidades contenidas en su legislación específica, se regirá por las disposiciones aplicables a dichas entidades en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a excepción de lo dispuesto en los artículos 103.1 y 107.3 de la Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional vigesimoquinta. *Régimen jurídico aplicable a los administradores generales de infraestructuras ferroviarias.*

Los administradores generales de infraestructuras ferroviarias preservarán su naturaleza de entidades públicas empresariales y, con las especialidades contenidas en su legislación propia, se regirán por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector del Sector Público a excepción de lo dispuesto en los artículos 103.1 y 107.3 de dicha Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional vigesimosexta. *Régimen jurídico aplicable a SEPES, Entidad Pública Empresarial del Suelo.*

SEPES, Entidad Pública Empresarial de Suelo, preservará su naturaleza de entidad pública empresarial y, con las especialidades contenidas en su legislación específica, se regirá por las disposiciones aplicables a dichas entidades en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a excepción de lo dispuesto en los artículos 103.1 y 107.3 de la Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional vigesimoséptima. *Régimen jurídico aplicable a la Entidad Pública Empresarial Red.es.*

La Entidad Pública Empresarial Red.es preservará su naturaleza de entidad pública empresarial y, con las especialidades contenidas en su legislación específica, se regirá por las disposiciones aplicables a dichas entidades en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a excepción de lo dispuesto en los artículos 103.1 y 107.3 de la Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional vigesimoctava. *Régimen jurídico aplicable a la entidad pública empresarial Instituto para la Diversificación y Ahorro de la Energía.*

El Instituto para la Diversificación y Ahorro de la Energía (IDAE) preservará su naturaleza de entidad pública empresarial y, con las especialidades contenidas en su legislación específica, se regirá por las disposiciones aplicables a dichas entidades en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a excepción de lo dispuesto en los

artículos 103.1 y 107.3 de la Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional vigesimonovena. *Régimen jurídico aplicable a la Entidad Pública Empresarial ICEX España Exportación e Inversiones.*

La Entidad Pública Empresarial ICEX España Exportación e Inversiones preservará su naturaleza de entidad pública empresarial y, con las especialidades contenidas en su legislación específica, se regirá por las disposiciones aplicables a dichas entidades en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, a excepción de lo dispuesto en los artículos 103.1 y 107.3 de la Ley, exclusivamente en lo que se refiere a la financiación mayoritaria con ingresos de mercado.

Disposición adicional trigésima. *Plataforma Digital de Colaboración entre las Administraciones Públicas.*

1. El Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Política Territorial impulsarán mediante orden ministerial conjunta las medidas necesarias para la creación y el funcionamiento de la Plataforma Digital de Colaboración entre las Administraciones Públicas como instrumento destinado a facilitar las relaciones y el soporte electrónico de los órganos integrantes del sistema de Conferencias Sectoriales y en general de los órganos de cooperación.

2. En aplicación del principio de colaboración, las Administraciones Públicas designarán los Puntos de Contacto correspondientes para atender las diversas funcionalidades de la Plataforma.

3. Reglamentariamente se regulará la configuración y régimen de funcionamiento de la Plataforma que, en cualquier caso, se adaptará a los criterios y directrices que sucesivamente establezca la Conferencia Sectorial de Administración Pública o, en su caso, la Comisión Sectorial de Administración Electrónica como órgano dependiente de aquélla.

Disposición transitoria primera. *Composición y clasificación del sector público institucional.*

La composición y clasificación del sector público institucional estatal prevista en el artículo 84 se aplicará únicamente a los organismos públicos y las entidades integrantes del sector público institucional estatal que se creen tras la entrada en vigor de la Ley y a los que se hayan adaptado de acuerdo con lo previsto en la disposición adicional cuarta.

Disposición transitoria segunda. *Entidades y organismos públicos existentes.*

1. Todos los organismos y entidades integrantes del sector público estatal en el momento de la entrada en vigor de esta Ley continuarán rigiéndose por su normativa específica, incluida la normativa presupuestaria que les resultaba de aplicación, hasta su adaptación a lo dispuesto en la Ley de acuerdo con lo previsto en la disposición adicional cuarta.

2. No obstante, en tanto no resulte contrario a su normativa específica:

a) Los organismos públicos existentes en el momento de la entrada en vigor de esta Ley y desde ese momento aplicarán los principios establecidos en el Capítulo I del Título II, el régimen de control previsto en el artículo 85 y 92.2, y lo dispuesto en los artículos 87, 94, 96, 97 si se transformaran fusionaran, disolvieran o liquidaran tras la entrada en vigor de esta Ley.

b) Las sociedades mercantiles estatales, los consorcios, fundaciones y fondos sin personalidad jurídica existentes en el momento de la entrada en vigor de esta Ley aplicarán desde ese momento, respectivamente, lo previsto en el Capítulo V, Capítulo VI, Capítulo VII y Capítulo VIII del Título II.

Disposición transitoria tercera. *Procedimientos de elaboración de normas en la Administración General del Estado.*

Los procedimientos de elaboración de normas que se hallaren en tramitación en la Administración General del Estado a la entrada en vigor de esta Ley se sustanciarán de acuerdo con lo establecido en la normativa vigente en el momento en que se iniciaron.

Disposición transitoria cuarta. *Régimen transitorio de las modificaciones introducidas en la disposición final novena.*

Lo dispuesto en la disposición final novena será de aplicación a los expedientes de contratación iniciados con posterioridad a la entrada en vigor de dicha disposición. A estos efectos se entenderá que los expedientes de contratación han sido iniciados si se hubiera publicado la correspondiente convocatoria del procedimiento de adjudicación del contrato. En el caso de procedimientos negociados, para determinar el momento de iniciación se tomará en cuenta la fecha de aprobación de los pliegos.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan, contradigan o resulten incompatibles con lo dispuesto en la presente Ley y, en especial:

a) El artículo 87 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
b) El artículo 110 del texto refundido de las disposiciones legales vigentes en materia de Régimen Local aprobado por el Real Decreto Legislativo 781/1986, de 18 de abril.
c) Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.
d) Los artículos 44, 45 y 46 de la Ley 50/2002, de 26 de diciembre, de Fundaciones.
e) Ley 28/2006, de 18 de julio, de Agencias estatales para la mejora de los servicios públicos.
f) Los artículos 12, 13, 14 y 15 y disposición adicional sexta de la Ley 15/2014, de 16 de septiembre, de racionalización del Sector Público y otras medidas de reforma administrativa.
g) El artículo 6.1.f), la disposición adicional tercera, la disposición transitoria segunda y la disposición transitoria cuarta del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
h) Los artículos 37, 38, 39 y 40 del Decreto de 17 de junio de 1955 por el que se aprueba el Reglamento de Servicios de las Corporaciones locales.

Hasta que, de acuerdo con lo previsto en la disposición adicional cuarta, concluya el plazo de adaptación de las agencias existentes en el sector público estatal, se mantendrá en vigor la Ley 28/2006, de 18 de julio.

Disposición final primera. *Modificación de la Ley 23/1982, de 16 de junio, reguladora del Patrimonio Nacional.*

El apartado uno del artículo octavo de la Ley 23/1982, de 16 de junio, reguladora del Patrimonio Nacional, quedará redactado en la forma siguiente:

> «Uno. El Consejo de Administración del Patrimonio Nacional estará constituido por su Presidente, el Gerente y por un número de Vocales no superior a trece, todos los cuales deberán ser profesionales de reconocido prestigio. Al Presidente y al Gerente les será de aplicación lo establecido en el artículo 2 de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del Alto Cargo de la Administración General del Estado, debiendo realizarse su nombramiento entre funcionarios de carrera del Estado, de las Comunidades Autónomas o de las Entidades Locales, pertenecientes a cuerpos clasificados en el Subgrupo A1.
>
> Dos de los Vocales, al menos, deberán de provenir de instituciones museísticas y culturales de reconocido prestigio y proyección internacional. Igualmente, en dos de los Vocales, al menos, habrá de concurrir la condición de Alcaldes de Ayuntamientos

en cuyo término municipal radiquen bienes inmuebles históricos del Patrimonio Nacional.

El Presidente, el Gerente y los demás miembros del Consejo de Administración serán nombrados mediante Real Decreto, previa deliberación del Consejo de Ministros a propuesta del Presidente del Gobierno.»

Disposición final segunda. *Modificación del Real Decreto-Ley 12/1995, de 28 de diciembre, sobre medidas urgentes en materia presupuestaria, tributaria y financiera.*

Uno. Se añade un nuevo apartado tres a la disposición adicional sexta, renumerándose los apartados tres a seis como cuatro a siete. El apartado tres tendrá la siguiente redacción:

«Tres. Consejo General.

1. El Instituto de Crédito Oficial estará regido por un Consejo General, que tendrá a su cargo la superior dirección de su administración y gestión.

2. El Consejo General estará formado por el Presidente de la entidad, que lo será también del Consejo, y diez Vocales, y estará asistido por el Secretario y, en su caso, el Vicesecretario del mismo.

Todos los integrantes del Consejo General actuarán siempre en interés del Instituto de Crédito Oficial en el ejercicio de sus funciones como miembros del Consejo General.

3. El nombramiento y cese de los Vocales del Consejo General corresponde al Consejo de Ministros, a propuesta del Ministro de Economía y Competitividad, que los designará entre personas de reconocido prestigio y competencia profesional en el ámbito de actividad del Instituto de Crédito Oficial.

4. Cuatro de los diez Vocales del Consejo serán independientes. A tal efecto, se entenderá independiente aquél que no sea personal al servicio del Sector Público.

5. El mandato de los vocales independientes será de tres años, tras el cual cabrá una sola reelección.

Reglamentariamente se establecerán las causas de cese de dichos Vocales, así como el régimen jurídico al que quedan sometidos los integrantes del Consejo General.

6. Cada uno de los Vocales independientes dispondrá de dos votos exclusivamente para la adopción de acuerdos relativos a operaciones financieras de activo y pasivo propias del negocio del Instituto.»

Dos. Se añade una nueva disposición transitoria, que tendrá la siguiente redacción:

«Disposición transitoria quinta. *Operaciones y atribuciones vigentes.*

La modificación de la disposición adicional sexta del Real Decreto-Ley 12/1995, de 28 de diciembre, introducida por la disposición final segunda de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, no afectará al régimen de las operaciones del Instituto de Crédito Oficial actualmente en vigor, sin que por ello se modifiquen los términos y condiciones de los contratos y convenios suscritos.

Adicionalmente, se mantendrán las atribuciones, poderes y delegaciones conferidas por el Consejo General en otras autoridades y órganos del Instituto de Crédito Oficial hasta que el Consejo General decida, en su caso, su revisión.

Los Consejeros que, a la entrada en vigor de la disposición final segunda de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, formasen parte del Consejo General del Instituto de Crédito Oficial continuarán en el ejercicio de sus funciones hasta que se nombre a quienes hubieran de sucederles.»

Disposición final tercera. *Modificación de la Ley 50/1997, de 27 de noviembre, del Gobierno.*

La Ley 50/1997, de 27 de noviembre, del Gobierno, queda modificada en los siguientes términos:

Uno. El apartado segundo del artículo 4 queda redactado en los siguientes términos:

«2. Además de los Ministros titulares de un Departamento, podrán existir Ministros sin cartera, a los que se les atribuirá la responsabilidad de determinadas funciones gubernamentales. En caso de que existan Ministros sin cartera, por Real Decreto se determinará el ámbito de sus competencias, la estructura administrativa, así como los medios materiales y personales que queden adscritos al mismo.»

Dos. Se modifica el artículo 5 que queda redactado en los siguientes términos:

«Artículo 5. *Del Consejo de Ministros.*

1. Al Consejo de Ministros, como órgano colegiado del Gobierno, le corresponde el ejercicio de las siguientes funciones:

a) Aprobar los proyectos de ley y su remisión al Congreso de los Diputados o, en su caso, al Senado.
b) Aprobar el Proyecto de Ley de Presupuestos Generales del Estado.
c) Aprobar los Reales Decretos-leyes y los Reales Decretos Legislativos.
d) Acordar la negociación y firma de Tratados internacionales, así como su aplicación provisional.
e) Remitir los Tratados internacionales a las Cortes Generales en los términos previstos en los artículos 94 y 96.2 de la Constitución.
f) Declarar los estados de alarma y de excepción y proponer al Congreso de los Diputados la declaración del estado de sitio.
g) Disponer la emisión de Deuda Pública o contraer crédito, cuando haya sido autorizado por una Ley.
h) Aprobar los reglamentos para el desarrollo y la ejecución de las leyes, previo dictamen del Consejo de Estado, así como las demás disposiciones reglamentarias que procedan.
i) Crear, modificar y suprimir los órganos directivos de los Departamentos Ministeriales.
j) Adoptar programas, planes y directrices vinculantes para todos los órganos de la Administración General del Estado.
k) Ejercer cuantas otras atribuciones le confieran la Constitución, las leyes y cualquier otra disposición.

2. A las reuniones del Consejo de Ministros podrán asistir los Secretarios de Estado y excepcionalmente otros altos cargos, cuando sean convocados para ello.
3. Las deliberaciones del Consejo de Ministros serán secretas.»

Tres. El apartado segundo del artículo 6 queda redactado en los siguientes términos:

«2. El Real Decreto de creación de una Comisión Delegada deberá especificar, en todo caso:

a) El miembro del Gobierno que asume la presidencia de la Comisión.
b) Los miembros del Gobierno y, en su caso, Secretarios de Estado que la integran.
c) Las funciones que se atribuyen a la Comisión.
d) El miembro de la Comisión al que corresponde la Secretaría de la misma.
e) El régimen interno de funcionamiento y en particular el de convocatorias y suplencias.»

Cuatro. El apartado segundo del artículo 7 queda redactado en los siguientes términos:

«2. Actúan bajo la dirección del titular del Departamento al que pertenezcan. Cuando estén adscritos a la Presidencia del Gobierno, actúan bajo la dirección del Presidente.»

Cinco. El artículo 8 queda redactado en los siguientes términos:

«Artículo 8. *De la Comisión General de Secretarios de Estado y Subsecretarios.*

1. La Comisión General de Secretarios de Estado y Subsecretarios estará integrada por los titulares de las Secretarías de Estado y por los Subsecretarios de los distintos Departamentos Ministeriales.

Asistirá igualmente el Abogado General del Estado y aquellos altos cargos con rango de Secretario de Estado o Subsecretario que sean convocados por el Presidente por razón de la materia de que se trate.

2. La Presidencia de la Comisión General de Secretarios de Estado y Subsecretarios corresponde a un Vicepresidente del Gobierno o, en su defecto, al Ministro de la Presidencia. En caso de ausencia del Presidente de la Comisión, la presidencia recaerá en el Ministro que corresponda según el orden de precedencia de los Departamentos ministeriales. No se entenderá por ausencia la interrupción transitoria en la asistencia a la reunión de la Comisión. En ese caso, las funciones que pudieran corresponder al Presidente serán ejercidas por la siguiente autoridad en rango presente, de conformidad con el orden de precedencia de los distintos Departamentos ministeriales.

3. La Secretaría de la Comisión General de Secretarios de Estado y Subsecretarios será ejercida por el Subsecretario de la Presidencia. En caso de ausencia, vacante o enfermedad, actuará como Secretario el Director del Secretariado del Gobierno.

4. Las deliberaciones de la Comisión General de Secretarios de Estado y Subsecretarios serán reservadas. En ningún caso la Comisión podrá adoptar decisiones o acuerdos por delegación del Gobierno.

5. Corresponde a la Comisión General de Secretarios de Estado y Subsecretarios:

a) El examen de todos los asuntos que vayan a someterse a aprobación del Consejo de Ministros, excepto los nombramientos, ceses, ascensos a cualquiera de los empleos de la categoría de oficiales generales y aquéllos que, excepcionalmente y por razones de urgencia, deban ser sometidos directamente al Consejo de Ministros.

b) El análisis o discusión de aquellos asuntos que, sin ser competencia del Consejo de Ministros o sus Comisiones Delegadas, afecten a varios Ministerios y sean sometidos a la Comisión por su presidente.»

Seis. Se modifica el artículo 9 que queda redactado en los siguientes términos:

«Artículo 9. *Del Secretariado del Gobierno.*

1. El Secretariado del Gobierno, como órgano de apoyo del Consejo de Ministros, de las Comisiones Delegadas del Gobierno y de la Comisión General de Secretarios de Estado y Subsecretarios, ejercerá las siguientes funciones:

a) La asistencia al Ministro-Secretario del Consejo de Ministros.

b) La remisión de las convocatorias a los diferentes miembros de los órganos colegiados anteriormente enumerados.

c) La colaboración con las Secretarías Técnicas de las Comisiones Delegadas del Gobierno.

d) El archivo y custodia de las convocatorias, órdenes del día y actas de las reuniones.

e) Velar por el cumplimiento de los principios de buena regulación aplicables a las iniciativas normativas y contribuir a la mejora de la calidad técnica de las disposiciones aprobadas por el Gobierno.

f) Velar por la correcta y fiel publicación de las disposiciones y normas emanadas del Gobierno que deban insertarse en el "Boletín Oficial del Estado".

2. Asimismo, el Secretariado del Gobierno, como órgano de asistencia al Ministro de la Presidencia, ejercerá las siguientes funciones:

a) Los trámites relativos a la sanción y promulgación real de las leyes aprobadas por las Cortes Generales y la expedición de los Reales Decretos.

b) La tramitación de los actos y disposiciones del Rey cuyo refrendo corresponde al Presidente del Gobierno.

c) La tramitación de los actos y disposiciones que el ordenamiento jurídico atribuye a la competencia del Presidente del Gobierno.

3. El Secretariado del Gobierno se integra en la estructura orgánica del Ministerio de la Presidencia, tal como se prevea en el Real Decreto de estructura de ese Ministerio. El Director del Secretariado del Gobierno ejercerá la secretaría adjunta de la Comisión General de Secretarios de Estado y Subsecretarios.

4. De conformidad con las funciones que tiene atribuidas y de acuerdo con las normas que rigen la elaboración de las disposiciones de carácter general, el Secretariado del Gobierno propondrá al Ministro de la Presidencia la aprobación de las instrucciones que han de seguirse para la tramitación de asuntos ante los órganos colegiados del Gobierno y los demás previstos en el apartado segundo de este artículo. Las instrucciones preverán expresamente la forma de documentar las propuestas y acuerdos adoptados por medios electrónicos, que deberán asegurar la identidad de los órganos intervinientes y la fehaciencia del contenido.»

Siete. El artículo 10 queda redactado en los siguientes términos:

«10. De los Gabinetes.

1. Los Gabinetes son órganos de apoyo político y técnico del Presidente del Gobierno, de los Vicepresidentes, de los Ministros y de los Secretarios de Estado. Los miembros de los Gabinetes realizan tareas de confianza y asesoramiento especial sin que en ningún caso puedan adoptar actos o resoluciones que correspondan legalmente a los órganos de la Administración General del Estado o de las organizaciones adscritas a ella, sin perjuicio de su asistencia o pertenencia a órganos colegiados que adopten decisiones administrativas. Asimismo, los directores de los gabinetes podrán dictar los actos administrativos propios de la jefatura de la unidad que dirigen.

Particularmente, los Gabinetes prestan su apoyo a los miembros del Gobierno y Secretarios de Estado en el desarrollo de su labor política, en el cumplimiento de las tareas de carácter parlamentario y en sus relaciones con las instituciones y la organización administrativa.

El Gabinete de la Presidencia del Gobierno se regulará por Real Decreto del Presidente en el que se determinará, entre otros aspectos, su estructura y funciones. El resto de Gabinetes se regulará por lo dispuesto en esta Ley.

2. Los Directores de Gabinete tendrán el nivel orgánico que se determine reglamentariamente. El resto de miembros del Gabinete tendrán la situación y grado administrativo que les corresponda en virtud de la legislación correspondiente.

3. Las retribuciones de los miembros de los Gabinetes se determinan por el Consejo de Ministros dentro de las consignaciones presupuestarias establecidas al efecto adecuándose, en todo caso, a las retribuciones de la Administración General del Estado.»

Ocho. Se modifica el artículo 11 con la siguiente redacción:

«Artículo 11. *De los requisitos de acceso al cargo.*

Para ser miembro del Gobierno se requiere ser español, mayor de edad, disfrutar de los derechos de sufragio activo y pasivo, así como no estar inhabilitado para ejercer empleo o cargo público por sentencia judicial firme y reunir el resto de requisitos de idoneidad previstos en la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.»

Nueve. El artículo 12 queda redactado en los siguientes términos:

«Artículo 12. *Del nombramiento y cese.*

1. El nombramiento y cese del Presidente del Gobierno se producirá en los términos previstos en la Constitución.

2. Los Vicepresidentes y Ministros serán nombrados y separados por el Rey, a propuesta del Presidente del Gobierno. El nombramiento conllevará el cese en el puesto que, en su caso, se estuviera desempeñando, salvo cuando en el caso de los Vicepresidentes, se designe como tal a un Ministro que conserve la titularidad del Departamento. Cuando el cese en el anterior cargo correspondiera al Consejo de Ministros, se dejará constancia de esta circunstancia en el nombramiento del nuevo titular. La separación de los Ministros sin cartera llevará aparejada la extinción de dichos órganos.

3. La separación de los Vicepresidentes del Gobierno llevará aparejada la extinción de dichos órganos, salvo el caso en que simultáneamente se designe otro vicepresidente en sustitución del separado.

4. Por Real Decreto se regulará el estatuto que fuera aplicable a los Presidentes del Gobierno tras su cese.»

Diez. El artículo 13 queda redactado en los siguientes términos:

«Artículo 13. *De la suplencia.*

1. En los casos de vacante, ausencia o enfermedad, las funciones del Presidente del Gobierno serán asumidas por los Vicepresidentes, de acuerdo con el correspondiente orden de prelación, y, en defecto de ellos, por los Ministros, según el orden de precedencia de los Departamentos.

2. La suplencia de los Ministros, para el despacho ordinario de los asuntos de su competencia, será determinada por Real Decreto del Presidente del Gobierno, debiendo recaer, en todo caso, en otro miembro del Gobierno. El Real Decreto expresará entre otras cuestiones la causa y el carácter de la suplencia.

3. No se entenderá por ausencia la interrupción transitoria de la asistencia a la reunión de un órgano colegiado. En tales casos, las funciones que pudieran corresponder al miembro del gobierno durante esa situación serán ejercidas por la siguiente autoridad en rango presente.»

Once. El artículo 20 queda redactado en los siguientes términos:

«Artículo 20. *Delegación y avocación de competencias.*

1. Pueden delegar el ejercicio de competencias propias:

a) El Presidente del Gobierno en favor del Vicepresidente o Vicepresidentes y de los Ministros.

b) Los Ministros en favor de los Secretarios de Estado y de los Subsecretarios dependientes de ellos, de los Delegados del Gobierno en las Comunidades Autónomas y de los demás órganos directivos del Ministerio.

2. Asimismo, son delegables a propuesta del Presidente del Gobierno las funciones administrativas del Consejo de Ministros en las Comisiones Delegadas del Gobierno.

3. No son en ningún caso delegables las siguientes competencias:

a) Las atribuidas directamente por la Constitución.

b) Las relativas al nombramiento y separación de los altos cargos atribuidas al Consejo de Ministros.

c) Las atribuidas a los órganos colegiados del Gobierno, con la excepción prevista en el apartado 2 de este artículo.

d) Las atribuidas por una ley que prohíba expresamente la delegación.

4. El Consejo de Ministros podrá avocar para sí, a propuesta del Presidente del Gobierno, el conocimiento de un asunto cuya decisión corresponda a las Comisiones Delegadas del Gobierno.

La avocación se realizará mediante acuerdo motivado al efecto, del que se hará mención expresa en la decisión que se adopte en el ejercicio de la avocación. Contra el acuerdo de avocación no cabrá recurso, aunque podrá impugnarse en el que, en su caso, se interponga contra la decisión adoptada.»

Doce. El Título V queda redactado del siguiente modo:

«TÍTULO V

De la iniciativa legislativa y la potestad reglamentaria del Gobierno

Artículo 22. *Del ejercicio de la iniciativa legislativa y la potestad reglamentaria del Gobierno.*

El Gobierno ejercerá la iniciativa y la potestad reglamentaria de conformidad con los principios y reglas establecidos en el Título VI de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en el presente Título.

Artículo 23. *Disposiciones de entrada en vigor.*

Sin perjuicio de lo establecido en el artículo 2.1 del Código Civil, las disposiciones de entrada en vigor de las leyes o reglamentos, cuya aprobación o propuesta corresponda al Gobierno o a sus miembros, y que impongan nuevas obligaciones a las personas físicas o jurídicas que desempeñen una actividad económica o profesional como consecuencia del ejercicio de ésta, preverán el comienzo de su vigencia el 2 de enero o el 1 de julio siguientes a su aprobación.

Lo previsto en este artículo no será de aplicación a los reales decretos-leyes, ni cuando el cumplimiento del plazo de transposición de directivas europeas u otras razones justificadas así lo aconsejen, debiendo quedar este hecho debidamente acreditado en la respectiva Memoria.

Artículo 24. *De la forma y jerarquía de las disposiciones y resoluciones del Gobierno de la Nación y de sus miembros.*

1. Las decisiones del Gobierno de la Nación y de sus miembros revisten las formas siguientes:

a) Reales Decretos Legislativos y Reales Decretos-leyes, las decisiones que aprueban, respectivamente, las normas previstas en los artículos 82 y 86 de la Constitución.

b) Reales Decretos del Presidente del Gobierno, las disposiciones y actos cuya adopción venga atribuida al Presidente.

c) Reales Decretos acordados en Consejo de Ministros, las decisiones que aprueben normas reglamentarias de la competencia de éste y las resoluciones que deban adoptar dicha forma jurídica.

d) Acuerdos del Consejo de Ministros, las decisiones de dicho órgano colegiado que no deban adoptar la forma de Real Decreto.

e) Acuerdos adoptados en Comisiones Delegadas del Gobierno, las disposiciones y resoluciones de tales órganos colegiados. Tales acuerdos revestirán la forma de Orden del Ministro competente o del Ministro de la Presidencia, cuando la competencia corresponda a distintos Ministros.

f) Órdenes Ministeriales, las disposiciones y resoluciones de los Ministros. Cuando la disposición o resolución afecte a varios Departamentos revestirá la forma de Orden del Ministro de la Presidencia, dictada a propuesta de los Ministros interesados.

2. Los reglamentos se ordenarán según la siguiente jerarquía:

1.º Disposiciones aprobadas por Real Decreto del Presidente del Gobierno o acordado en el Consejo de Ministros.

2.º Disposiciones aprobadas por Orden Ministerial.

Artículo 25. *Plan Anual Normativo.*

1. El Gobierno aprobará anualmente un Plan Normativo que contendrá las iniciativas legislativas o reglamentarias que vayan a ser elevadas para su aprobación en el año siguiente.

2. El Plan Anual Normativo identificará, con arreglo a los criterios que se establezcan reglamentariamente, las normas que habrán de someterse a un análisis sobre los resultados de su aplicación, atendiendo fundamentalmente al coste que suponen para la Administración o los destinatarios y las cargas administrativas impuestas a estos últimos.

3. Cuando se eleve para su aprobación por el órgano competente una propuesta normativa que no figurara en el Plan Anual Normativo al que se refiere el presente artículo será necesario justificar este hecho en la correspondiente Memoria del Análisis de Impacto Normativo.

4. El Plan Anual Normativo estará coordinado por el Ministerio de la Presidencia, con el objeto de asegurar la congruencia de todas las iniciativas que se tramiten y de evitar sucesivas modificaciones del régimen legal aplicable a un determinado sector o área de actividad en un corto espacio de tiempo. El Ministro de la Presidencia elevará el Plan al Consejo de Ministros para su aprobación antes del 30 de abril.

Por orden del Ministerio de la Presidencia se aprobarán los modelos que contengan la información a remitir sobre cada iniciativa normativa para su inclusión en el Plan.

Artículo 26. *Procedimiento de elaboración de normas con rango de Ley y reglamentos.*

La elaboración de los anteproyectos de ley, de los proyectos de real decreto legislativo y de normas reglamentarias se ajustará al siguiente procedimiento:

1. Su redacción estará precedida de cuantos estudios y consultas se estimen convenientes para garantizar el acierto y la legalidad de la norma.

2. Se sustanciará una consulta pública, a través del portal web del departamento competente, con carácter previo a la elaboración del texto, en la que se recabará opinión de los sujetos potencialmente afectados por la futura norma y de las organizaciones más representativas acerca de:

a) Los problemas que se pretenden solucionar con la nueva norma.
b) La necesidad y oportunidad de su aprobación.
c) Los objetivos de la norma.
d) Las posibles soluciones alternativas regulatorias y no regulatorias.

Podrá prescindirse del trámite de consulta pública previsto en este apartado en el caso de la elaboración de normas presupuestarias u organizativas de la Administración General del Estado o de las organizaciones dependientes o vinculadas a éstas, cuando concurran razones graves de interés público que lo justifiquen, o cuando la propuesta normativa no tenga un impacto significativo en la actividad económica, no imponga obligaciones relevantes a los destinatarios o regule aspectos parciales de una materia. También podrá prescindirse de este trámite de consulta en el caso de tramitación urgente de iniciativas normativas, tal y como se establece en el artículo 27.2. La concurrencia de alguna o varias de estas razones, debidamente motivadas, se justificarán en la Memoria del Análisis de Impacto Normativo.

La consulta pública deberá realizarse de tal forma que todos los potenciales destinatarios de la norma tengan la posibilidad de emitir su opinión, para lo cual deberá proporcionarse un tiempo suficiente, que en ningún caso será inferior a quince días naturales.

3. El centro directivo competente elaborará con carácter preceptivo una Memoria del Análisis de Impacto Normativo, que deberá contener los siguientes apartados:

a) Oportunidad de la propuesta y alternativas de regulación estudiadas, lo que deberá incluir una justificación de la necesidad de la nueva norma frente a la alternativa de no aprobar ninguna regulación.

b) Contenido y análisis jurídico, con referencia al Derecho nacional y de la Unión Europea, que incluirá el listado pormenorizado de las normas que quedarán derogadas como consecuencia de la entrada en vigor de la norma.

c) Análisis sobre la adecuación de la norma propuesta al orden de distribución de competencias.

d) Impacto económico y presupuestario, que evaluará las consecuencias de su aplicación sobre los sectores, colectivos o agentes afectados por la norma, incluido el efecto sobre la competencia, la unidad de mercado y la competitividad y su encaje con la legislación vigente en cada momento sobre estas materias. Este análisis incluirá la realización del test Pyme de acuerdo con la práctica de la Comisión Europea.

e) Asimismo, se identificarán las cargas administrativas que conlleva la propuesta, se cuantificará el coste de su cumplimiento para la Administración y para los obligados a soportarlas con especial referencia al impacto sobre las pequeñas y medianas empresas.

f) Impacto por razón de género, que analizará y valorará los resultados que se puedan seguir de la aprobación de la norma desde la perspectiva de la eliminación de desigualdades y de su contribución a la consecución de los objetivos de igualdad de oportunidades y de trato entre mujeres y hombres, a partir de los indicadores de situación de partida, de previsión de resultados y de previsión de impacto.

g) Un resumen de las principales aportaciones recibidas en el trámite de consulta pública regulado en el apartado 2.

La Memoria del Análisis de Impacto Normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente.

4. Cuando la disposición normativa sea un anteproyecto de ley o un proyecto de real decreto legislativo, cumplidos los trámites anteriores, el titular o titulares de los Departamentos proponentes lo elevarán, previo sometimiento a la Comisión General de Secretarios de Estado y Subsecretarios, al Consejo de Ministros, a fin de que éste decida sobre los ulteriores trámites y, en particular, sobre las consultas, dictámenes e informes que resulten convenientes, así como sobre los términos de su realización, sin perjuicio de los legalmente preceptivos.

Cuando razones de urgencia así lo aconsejen, y siempre que se hayan cumplimentado los trámites de carácter preceptivo, el Consejo de Ministros podrá prescindir de este y acordar la aprobación del anteproyecto de ley o proyecto de real decreto legislativo y su remisión, en su caso, al Congreso de los Diputados o al Senado, según corresponda.

5. A lo largo del procedimiento de elaboración de la norma, el centro directivo competente recabará, además de los informes y dictámenes que resulten preceptivos, cuantos estudios y consultas se estimen convenientes para garantizar el acierto y la legalidad del texto.

Salvo que normativamente se establezca otra cosa, los informes preceptivos se emitirán en un plazo de diez días, o de un mes cuando el informe se solicite a otra Administración o a un órgano u Organismo dotado de especial independencia o autonomía.

El centro directivo competente podrá solicitar motivadamente la emisión urgente de los informes, estudios y consultas solicitados, debiendo éstos ser emitidos en un plazo no superior a la mitad de la duración de los indicados en el párrafo anterior.

En todo caso, los anteproyectos de ley, los proyectos de real decreto legislativo y los proyectos de disposiciones reglamentarias, deberán ser informados por la Secretaría General Técnica del Ministerio o Ministerios proponentes.

Asimismo, cuando la propuesta normativa afectara a la organización administrativa de la Administración General del Estado, a su régimen de personal, a los procedimientos y a la inspección de los servicios, será necesario recabar la aprobación previa del Ministerio de Hacienda y Administraciones Públicas antes de

ser sometidas al órgano competente para promulgarlos. Si transcurridos 15 días desde la recepción de la solicitud de aprobación por parte del citado Ministerio no se hubiera formulado ninguna objeción, se entenderá concedida la aprobación.

Será además necesario informe previo del Ministerio de Hacienda y Administraciones Públicas cuando la norma pudiera afectar a la distribución de las competencias entre el Estado y las Comunidades Autónomas.

6. Sin perjuicio de la consulta previa a la redacción del texto de la iniciativa, cuando la norma afecte a los derechos e intereses legítimos de las personas, el centro directivo competente publicará el texto en el portal web correspondiente, con el objeto de dar audiencia a los ciudadanos afectados y obtener cuantas aportaciones adicionales puedan hacerse por otras personas o entidades. Asimismo, podrá recabarse directamente la opinión de las organizaciones o asociaciones reconocidas por ley que agrupen o representen a las personas cuyos derechos o intereses legítimos se vieren afectados por la norma y cuyos fines guarden relación directa con su objeto.

El plazo mínimo de esta audiencia e información públicas será de 15 días hábiles, y podrá ser reducido hasta un mínimo de siete días hábiles cuando razones debidamente motivadas así lo justifiquen; así como cuando se aplique la tramitación urgente de iniciativas normativas, tal y como se establece en el artículo 27.2. De ello deberá dejarse constancia en la Memoria del Análisis de Impacto Normativo.

El trámite de audiencia e información pública sólo podrá omitirse cuando existan graves razones de interés público, que deberán justificarse en la Memoria del Análisis de Impacto Normativo. Asimismo, no será de aplicación a las disposiciones presupuestarias o que regulen los órganos, cargos y autoridades del Gobierno o de las organizaciones dependientes o vinculadas a éstas.

7. Se recabará el dictamen del Consejo de Estado u órgano consultivo equivalente cuando fuera preceptivo o se considere conveniente.

8. Cumplidos los trámites anteriores, la propuesta se someterá a la Comisión General de Secretarios de Estado y Subsecretarios y se elevará al Consejo de Ministros para su aprobación y, en caso de proyectos de ley, su remisión al Congreso de los Diputados o, en su caso, al Senado, acompañándolo de una Exposición de Motivos y de la documentación propia del procedimiento de elaboración a que se refieren las letras b) y d) del artículo 7 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y su normativa de desarrollo.

9. El Ministerio de la Presidencia, con el objeto de asegurar la coordinación y la calidad de la actividad normativa del Gobierno analizará los siguientes aspectos:

a) La calidad técnica y el rango de la propuesta normativa.

b) La congruencia de la iniciativa con el resto del ordenamiento jurídico, nacional y de la Unión Europea, con otras que se estén elaborando en los distintos Ministerios o que vayan a hacerlo de acuerdo con el Plan Anual Normativo, así como con las que se estén tramitando en las Cortes Generales.

c) La necesidad de incluir la derogación expresa de otras normas, así como de refundir en la nueva otras existentes en el mismo ámbito.

d) El contenido preceptivo de la Memoria del Análisis de Impacto Normativo y, en particular, la inclusión de una sistemática de evaluación posterior de la aplicación de la norma cuando fuere preceptivo.

e) El cumplimiento de los principios y reglas establecidos en este Título.

f) El cumplimiento o congruencia de la iniciativa con los proyectos de reducción de cargas administrativas o buena regulación que se hayan aprobado en disposiciones o acuerdos de carácter general para la Administración General del Estado.

g) La posible extralimitación de la iniciativa normativa respecto del contenido de la norma comunitaria que se trasponga al derecho interno.

Reglamentariamente se determinará la composición del órgano encargado de la realización de esta función así como su modo de intervención en el procedimiento.

10. Se conservarán en el correspondiente expediente administrativo, en formato electrónico, la Memoria del Análisis de Impacto Normativo, los informes y dictámenes recabados para su tramitación, así como todos los estudios y consultas emitidas y demás actuaciones practicadas.

11. Lo dispuesto en este artículo y en el siguiente no será de aplicación para la tramitación y aprobación de decretos-leyes, a excepción de la elaboración de la memoria prevista en el apartado 3, con carácter abreviado, y lo establecido en los números 1, 8, 9 y 10.

Artículo 27. *Tramitación urgente de iniciativas normativas en el ámbito de la Administración General del Estado.*

1. El Consejo de Ministros, a propuesta del titular del departamento al que corresponda la iniciativa normativa, podrá acordar la tramitación urgente del procedimiento de elaboración y aprobación de anteproyectos de ley, reales decretos legislativos y de reales decretos, en alguno de los siguientes casos:

a) Cuando fuere necesario para que la norma entre en vigor en el plazo exigido para la transposición de directivas comunitarias o el establecido en otras leyes o normas de Derecho de la Unión Europea.

b) Cuando concurran otras circunstancias extraordinarias que, no habiendo podido preverse con anterioridad, exijan la aprobación urgente de la norma.

La Memoria del Análisis de Impacto Normativo que acompañe al proyecto mencionará la existencia del acuerdo de tramitación urgente, así como las circunstancias que le sirven de fundamento.

2. La tramitación por vía de urgencia implicará que:

a) Los plazos previstos para la realización de los trámites del procedimiento de elaboración, establecidos en ésta o en otra norma, se reducirán a la mitad de su duración. Si, en aplicación de la normativa reguladora de los órganos consultivos que hubieran de emitir dictamen, fuera necesario un acuerdo para requerirlo en dicho plazo, se adoptará por el órgano competente; y si fuera el Consejo de Ministros, se recogerá en el acuerdo previsto en el apartado 1 de este artículo.

b) No será preciso el trámite de consulta pública previsto en el artículo 26.2, sin perjuicio de la realización de los trámites de audiencia pública o de información pública sobre el texto a los que se refiere el artículo 26.6, cuyo plazo de realización será de siete días.

c) La falta de emisión de un dictamen o informe preceptivo en plazo no impedirá la continuación del procedimiento, sin perjuicio de su eventual incorporación y consideración cuando se reciba.

Artículo 28. *Informe anual de evaluación.*

1. El Consejo de Ministros, a propuesta del Ministerio de la Presidencia, aprobará, antes del 30 de abril de cada año, un informe anual en el que se refleje el grado de cumplimiento del Plan Anual Normativo del año anterior, las iniciativas adoptadas que no estaban inicialmente incluidas en el citado Plan, así como las incluidas en anteriores informes de evaluación con objetivos plurianuales que hayan producido al menos parte de sus efectos en el año que se evalúa.

2. En el informe se incluirán las conclusiones del análisis de la aplicación de las normas a que se refiere el artículo 25.2, que, de acuerdo con lo previsto en su respectiva Memoria, hayan tenido que ser evaluadas en el ejercicio anterior. La evaluación se realizará en los términos y plazos previstos en la Memoria del Análisis de Impacto Normativo y deberá comprender, en todo caso:

a) La eficacia de la norma, entendiendo por tal la medida en que ha conseguido los fines pretendidos con su aprobación.

b) La eficiencia de la norma, identificando las cargas administrativas que podrían no haber sido necesarias.

c) La sostenibilidad de la disposición.

El informe podrá contener recomendaciones específicas de modificación y, en su caso, derogación de las normas evaluadas, cuando así lo aconsejase el resultado del análisis.»

Trece. Se añade un Título VI en el que se incluye el artículo 26 actual, que se renumera como artículo 29, y que queda redactado del siguiente modo:

«TÍTULO VI

Del control del Gobierno

Artículo 29. *Del control de los actos del Gobierno.*

1. El Gobierno está sujeto a la Constitución y al resto del ordenamiento jurídico en toda su actuación.

2. Todos los actos y omisiones del Gobierno están sometidos al control político de las Cortes Generales.

3. Los actos, la inactividad y las actuaciones materiales que constituyan una vía de hecho del Gobierno y de los órganos y autoridades regulados en la presente Ley son impugnables ante la jurisdicción contencioso-administrativa, de conformidad con lo dispuesto en su Ley reguladora.

4. La actuación del Gobierno es impugnable ante el Tribunal Constitucional en los términos de la Ley Orgánica reguladora del mismo.»

Disposición final cuarta. *Modificación de la Ley 50/2002, de 26 de diciembre, de Fundaciones.*

El apartado 2 del artículo 34 de la Ley 50/2002, de 26 de diciembre, de Fundaciones, queda redactado en los siguientes términos:

«2. Las funciones de Protectorado respecto de las fundaciones de competencia estatal serán ejercidas por la Administración General del Estado a través de un único órgano administrativo, en la forma que reglamentariamente se determine.»

Disposición final quinta. *Modificación de la Ley 22/2003, de 9 de julio, Concursal.*

(Derogada).

Disposición final sexta. *Modificación de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas.*

La Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas queda modificada en los siguientes términos:

Uno. El apartado 1 del artículo 166, queda redactado como sigue:

«1. Las disposiciones de este título serán de aplicación a las siguientes entidades:

a) Las entidades públicas empresariales, a las que se refiere la Sección 3.ª del capítulo III del Título II de la Ley de Régimen Jurídico del Sector Público.

b) Las entidades de Derecho público vinculadas a la Administración General del Estado o a sus organismos públicos cuyos ingresos provengan, al menos en un 50 por ciento, de operaciones realizadas en el mercado.

c) Las sociedades mercantiles estatales, entendiendo por tales aquellas sobre la que se ejerce control estatal:

1.º Bien porque la participación directa en su capital social de la Administración General del Estado o algunas de las entidades que, conforme a lo dispuesto en el artículo 84 de la Ley de Régimen Jurídico del Sector Público integran el sector público institucional estatal, incluidas las sociedades mercantiles estatales, sea superior al 50 por 100. Para la determinación de este porcentaje, se sumarán las participaciones correspondientes a la Administración General del Estado y a todas

las entidades integradas en el sector público institucional estatal, en el caso de que en el capital social participen varias de ellas.

2.º Bien porque la sociedad mercantil se encuentre en el supuesto previsto en el artículo 4 de la Ley 24/1988, de 28 de julio, del Mercado de Valores respecto de la Administración General del Estado o de sus organismos públicos vinculados o dependientes.»

Dos. El apartado segundo del artículo 167 queda redactado en los siguientes términos:

«2. Las entidades a que se refiere el párrafo c) del apartado 1 del artículo anterior ajustarán la gestión de su patrimonio al Derecho privado, sin perjuicio de las disposiciones de esta ley que les resulten expresamente de aplicación.»

Disposición final séptima. *Modificación de la Ley 38/2003, de 17 de noviembre, General de Subvenciones.*

Se introducen las siguientes modificaciones en la Ley 38/2003, de 17 de noviembre, General de Subvenciones:

Uno. Se modifica el artículo 10, que queda redactado como sigue:

«Artículo 10. *Órganos competentes para la concesión de subvenciones.*

1. Los Ministros y los Secretarios de Estado en la Administración General del Estado y los presidentes o directores de los organismos y las entidades públicas vinculados o dependientes de la Administración General del Estado, cualquiera que sea el régimen jurídico a que hayan de sujetar su actuación, son los órganos competentes para conceder subvenciones, en sus respectivos ámbitos, previa consignación presupuestaria para este fin.

2. No obstante lo dispuesto en el apartado anterior, para autorizar la concesión de subvenciones de cuantía superior a 12 millones de euros será necesario acuerdo del Consejo de Ministros o, en el caso de que así lo establezca la normativa reguladora de la subvención, de la Comisión Delegada del Gobierno para Asuntos Económicos.

En el caso de subvenciones concedidas en régimen de concurrencia competitiva, la autorización del Consejo de Ministros a que se refiere el párrafo anterior deberá obtenerse antes de la aprobación de la convocatoria cuya cuantía supere el citado límite.

La autorización a que se refiere el párrafo anterior no implicará la aprobación del gasto, que, en todo caso, corresponderá al órgano competente.

3. Las facultades para conceder subvenciones, a que se refiere este artículo, podrán ser objeto de desconcentración mediante real decreto acordado en Consejo de Ministros.

4. La competencia para conceder subvenciones en las corporaciones locales corresponde a los órganos que tengan atribuidas tales funciones en la legislación de régimen local.»

Dos. Se modifica el apartado 1 de la disposición adicional decimosexta con el siguiente contenido:

«1. Las fundaciones del sector público únicamente podrán conceder subvenciones cuando así se autorice a la correspondiente fundación de forma expresa mediante acuerdo del Ministerio de adscripción u órgano equivalente de la Administración a la que la fundación esté adscrita y sin perjuicio de lo dispuesto en el artículo 10.2.

La aprobación de las bases reguladoras, la autorización previa de la concesión, las funciones derivadas de la exigencia del reintegro y de la imposición de sanciones, así como las funciones de control y demás que comporten el ejercicio de potestades administrativas, serán ejercidas por los órganos de la Administración que financien en mayor proporción la subvención correspondiente; en caso de que no sea posible

identificar tal Administración, las funciones serán ejercidas por los órganos de la Administración que ejerza el Protectorado de la fundación.»

Tres. Se introduce una nueva disposición transitoria tercera con el siguiente contenido:

«Disposición transitoria tercera. *Convocatorias iniciadas y subvenciones concedidas con anterioridad a la entrada en vigor de la modificación de la Ley 38/2003, de 17 de noviembre, General de Subvenciones incluida en la disposición final séptima de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.*

Las subvenciones públicas que se concedan en régimen de concurrencia competitiva cuya convocatoria se hubiera aprobado con anterioridad a la entrada en vigor de la modificación del artículo 10 de la Ley General de Subvenciones, se regirán por la normativa anterior.»

Cuatro. Se introduce una nueva disposición adicional vigésima quinta con el siguiente contenido:

«Disposición adicional vigésima quinta. *Servicio Nacional de Coordinación Antifraude para la protección de los intereses financieros de la Unión Europea.*

1. El Servicio Nacional de Coordinación Antifraude, integrado en la Intervención General de la Administración del Estado, coordinará las acciones encaminadas a proteger los intereses financieros de la Unión Europea contra el fraude y dar cumplimiento al artículo 325 del Tratado de Funcionamiento de la Unión Europea y al artículo 3.4 del Reglamento (UE, Euratom) n.° 883/2013, del Parlamento Europeo y del Consejo relativo a las investigaciones efectuadas por la Oficina Europea de Lucha contra el Fraude (OLAF).

2. Corresponde al Servicio Nacional de Coordinación Antifraude:

a) Dirigir la creación y puesta en marcha de las estrategias nacionales y promover los cambios legislativos y administrativos necesarios para proteger los intereses financieros de la Unión Europea.

b) Identificar las posibles deficiencias de los sistemas nacionales para la gestión de fondos de la Unión Europea.

c) Establecer los cauces de coordinación e información sobre irregularidades y sospechas de fraude entre las diferentes instituciones nacionales y la OLAF.

d) Promover la formación para la prevención y lucha contra el fraude.

3. El Servicio Nacional de Coordinación Antifraude ejercerá sus competencias con plena independencia y deberá ser dotado con los medios adecuados para atender los contenidos y requerimientos establecidos por la OLAF.

4. El Servicio Nacional de Coordinación Antifraude estará asistido por un Consejo Asesor presidido por el Interventor General de la Administración del Estado e integrado por representantes de los ministerios, organismos y demás instituciones nacionales que tengan competencias en la gestión, control, prevención y lucha contra el fraude en relación con los intereses financieros de la Unión Europea. Su composición y funcionamiento se determinarán por Real Decreto.

5. Las autoridades, los titulares de los órganos del Estado, de las Comunidades Autónomas y de las Entidades Locales, así como los jefes o directores de oficinas públicas, organismos y otros entes públicos y quienes, en general, ejerzan funciones públicas o desarrollen su trabajo en dichas entidades deberán prestar la debida colaboración y apoyo al Servicio. El Servicio tendrá las mismas facultades que la OLAF para acceder a la información pertinente en relación con los hechos que se estén investigando.

6. El Servicio podrá concertar convenios con la OLAF para la transmisión de la información y para la realización de investigaciones.»

Disposición final octava. *Modificación de la Ley 47/2003, de 26 de noviembre, General Presupuestaria.*

Se modifica la Ley 47/2003, de 26 de noviembre, General Presupuestaria, que queda redactada como sigue:

Uno. Se modifica el artículo 2 que queda redactado en los siguientes términos:

«Artículo 2. *Sector público estatal.*

1. A los efectos de esta Ley forman parte del sector público estatal:

a) La Administración General del Estado.
b) El sector público institucional estatal.

2. Integran el sector público institucional estatal las siguientes entidades:

a) Los organismos públicos vinculados o dependientes de la Administración General del Estado, los cuales se clasifican en:

1.° Organismos autónomos.
2.° Entidades Públicas Empresariales.

b) Las autoridades administrativas independientes.
c) Las sociedades mercantiles estatales.
d) Los consorcios adscritos a la Administración General del Estado.
e) Las fundaciones del sector público adscritas a la Administración General del Estado.
f) Los fondos sin personalidad jurídica.
g) Las universidades públicas no transferidas.
h) Las entidades gestoras, servicios comunes y las mutuas colaboradoras con la Seguridad Social en su función pública de colaboración en la gestión de la Seguridad Social, así como sus centros mancomunados.
i) Cualesquiera organismos y entidades de derecho público vinculados o dependientes de la Administración General del Estado.

3. Los órganos con dotación diferenciada en los Presupuestos Generales del Estado que, careciendo de personalidad jurídica, no están integrados en la Administración General del Estado, forman parte del sector público estatal, regulándose su régimen económico-financiero por esta Ley, sin perjuicio de las especialidades que se establezcan en sus normas de creación, organización y funcionamiento. No obstante, su régimen de contabilidad y de control quedará sometido en todo caso a lo establecido en dichas normas, sin que les sea aplicable en dichas materias lo establecido en esta Ley.

Sin perjuicio de lo anterior, esta Ley no será de aplicación a las Cortes Generales, que gozan de autonomía presupuestaria de acuerdo con lo establecido en el artículo 72 de la Constitución; no obstante, se mantendrá la coordinación necesaria para la elaboración del Proyecto de Ley de Presupuestos Generales del Estado.»

Dos. Se modifica el artículo 3 que queda redactado como sigue:

«Artículo 3. *Sector público administrativo, empresarial y fundacional.*

A los efectos de esta Ley, el sector público estatal se divide en los siguientes:

1. El sector público administrativo, integrado por:

a) La Administración General del Estado, los organismos autónomos, las autoridades administrativas independientes, las universidades públicas no transferidas y las entidades gestoras, servicios comunes y las mutuas colaboradoras con la Seguridad Social, así como sus centros mancomunados, así como las entidades del apartado 3 del artículo anterior.

b) Cualesquiera organismos y entidades de derecho público vinculados o dependientes de la Administración General del Estado, los consorcios y los fondos sin personalidad jurídica, que cumplan alguna de las dos características siguientes:

1.ª Que su actividad principal no consista en la producción en régimen de mercado de bienes y servicios destinados al consumo individual o colectivo, o que efectúen operaciones de redistribución de la renta y de la riqueza nacional, en todo caso sin ánimo de lucro.

2.ª Que no se financien mayoritariamente con ingresos comerciales, entendiéndose como tales a los efectos de esta Ley, los ingresos, cualquiera que sea su naturaleza, obtenidos como contrapartida de las entregas de bienes o prestaciones de servicios.

2. El sector público empresarial, integrado por:

a) Las entidades públicas empresariales.

b) Las sociedades mercantiles estatales.

c) Cualesquiera organismos y entidades de derecho público vinculados o dependientes de la Administración General del Estado, los consorcios y los fondos sin personalidad jurídica no incluidos en el sector público administrativo.

3. El sector público fundacional, integrado por las fundaciones del sector público estatal.»

Disposición final novena. *Modificación del Texto Refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre.*

El Texto Refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, queda modificado como sigue:

Uno. El artículo 60 queda redactado del siguiente modo:

«Artículo 60. *Prohibiciones de contratar.*

1. No podrán contratar con las entidades previstas en el artículo 3 de la presente Ley con los efectos establecidos en el artículo 61 bis, las personas en quienes concurra alguna de las siguientes circunstancias:

a) Haber sido condenadas mediante sentencia firme por delitos de terrorismo, constitución o integración de una organización o grupo criminal, asociación ilícita, financiación ilegal de los partidos políticos, trata de seres humanos, corrupción en los negocios, tráfico de influencias, cohecho, prevaricación, fraudes, negociaciones y actividades prohibidas a los funcionarios, delitos contra la Hacienda Pública y la Seguridad Social, delitos contra los derechos de los trabajadores, malversación, blanqueo de capitales, delitos relativos a la ordenación del territorio y el urbanismo, la protección del patrimonio histórico y el medio ambiente, o a la pena de inhabilitación especial para el ejercicio de profesión, oficio, industria o comercio.

La prohibición de contratar alcanzará a las personas jurídicas que sean declaradas penalmente responsables, y a aquéllas cuyos administradores o representantes, lo sean de hecho o de derecho, vigente su cargo o representación y hasta su cese, se encontraran en la situación mencionada en este apartado.

b) Haber sido sancionadas con carácter firme por infracción grave en materia profesional, de falseamiento de la competencia, de integración laboral y de igualdad de oportunidades y no discriminación de las personas con discapacidad, o de extranjería, de conformidad con lo establecido en la normativa vigente; por infracción muy grave en materia medioambiental, de acuerdo con lo establecido en la Ley 21/2013, de 9 de diciembre, de evaluación ambiental; en la Ley 22/1988, de 28 de julio, de Costas; en la Ley 4/1989, de 27 de marzo, de Conservación de los Espacios Naturales y de la Flora y Fauna Silvestres; en la Ley 11/1997, de 24 de abril, de Envases y Residuos de Envases; en la Ley 10/1998, de 21 de abril, de Residuos; en el Texto Refundido de la Ley de Aguas, aprobado por Real Decreto Legislativo 1/2001, de 20 de julio, y en la Ley 16/2002, de 1 de julio, de Prevención y

Control Integrados de la Contaminación; o por infracción muy grave en materia laboral o social, de acuerdo con lo dispuesto en el Texto Refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, aprobado por el Real Decreto Legislativo 5/2000, de 4 de agosto, así como por la infracción grave prevista en el artículo 22.2 del citado texto.

c) Haber solicitado la declaración de concurso voluntario, haber sido declaradas insolventes en cualquier procedimiento, hallarse declaradas en concurso, salvo que en éste haya adquirido la eficacia un convenio, estar sujetos a intervención judicial o haber sido inhabilitados conforme a la Ley 22/2003, de 9 de julio, Concursal, sin que haya concluido el período de inhabilitación fijado en la sentencia de calificación del concurso.

d) No hallarse al corriente en el cumplimiento de las obligaciones tributarias o de Seguridad Social impuestas por las disposiciones vigentes, en los términos que reglamentariamente se determinen; o en el caso de empresas de 50 o más trabajadores, no cumplir el requisito de que al menos el 2 por ciento de sus empleados sean trabajadores con discapacidad, de conformidad con el artículo 42 del Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, en las condiciones que reglamentariamente se determinen.

En relación con el cumplimiento de sus obligaciones tributarias o con la Seguridad Social, se considerará que las empresas se encuentran al corriente en el mismo cuando las deudas estén aplazadas, fraccionadas o se hubiera acordado su suspensión con ocasión de la impugnación de tales deudas.

e) Haber incurrido en falsedad al efectuar la declaración responsable a que se refiere el artículo 146 o al facilitar cualesquiera otros datos relativos a su capacidad y solvencia, o haber incumplido, por causa que le sea imputable, la obligación de comunicar la información que corresponda en materia de clasificación y la relativa a los registros de licitadores y empresas clasificadas.

f) Estar afectado por una prohibición de contratar impuesta en virtud de sanción administrativa firme, con arreglo a lo previsto en la Ley 38/2003, de 17 de noviembre, General de Subvenciones, o en la Ley 58/2003, de 17 de diciembre, General Tributaria.

g) Estar incursa la persona física o los administradores de la persona jurídica en alguno de los supuestos de la Ley 5/2006, de 10 de abril, de Regulación de los Conflictos de Intereses de los Miembros del Gobierno y de los Altos Cargos de la Administración General del Estado o las respectivas normas de las Comunidades Autónomas, de la Ley 53/1984, de 26 de diciembre, de Incompatibilidades del Personal al Servicio de las Administraciones Públicas o tratarse de cualquiera de los cargos electivos regulados en la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, en los términos establecidos en la misma.

La prohibición alcanzará a las personas jurídicas en cuyo capital participen, en los términos y cuantías establecidas en la legislación citada, el personal y los altos cargos a que se refiere el párrafo anterior, así como los cargos electos al servicio de las mismas.

La prohibición se extiende igualmente, en ambos casos, a los cónyuges, personas vinculadas con análoga relación de convivencia afectiva, ascendientes y descendientes, así como a parientes en segundo grado por consanguineidad o afinidad de las personas a que se refieren los párrafos anteriores, cuando se produzca conflicto de intereses con el titular del órgano de contratación o los titulares de los órganos en que se hubiere delegado la facultad para contratar o los que ejerzan la sustitución del primero.

h) Haber contratado a personas respecto de las que se haya publicado en el "Boletín Oficial del Estado" el incumplimiento a que se refiere el artículo 18.6 de la Ley 5/2006, de 10 de abril, de Regulación de los Conflictos de Intereses de los Miembros del Gobierno y de los Altos Cargos de la Administración General del Estado o en las respectivas normas de las Comunidades Autónomas, por haber pasado a prestar servicios en empresas o sociedades privadas directamente

relacionadas con las competencias del cargo desempeñado durante los dos años siguientes a la fecha de cese en el mismo. La prohibición de contratar se mantendrá durante el tiempo que permanezca dentro de la organización de la empresa la persona contratada con el límite máximo de dos años a contar desde el cese como alto cargo.

2. Además de las previstas en el apartado anterior, son circunstancias que impedirán a los empresarios contratar con las entidades comprendidas en el artículo 3 de la presente Ley, en las condiciones establecidas en el artículo 61 bis las siguientes:

a) Haber retirado indebidamente su proposición o candidatura en un procedimiento de adjudicación, o haber imposibilitado la adjudicación del contrato a su favor por no cumplimentar lo establecido en el apartado 2 del artículo 151 dentro del plazo señalado mediando dolo, culpa o negligencia.

b) Haber dejado de formalizar el contrato, que ha sido adjudicado a su favor, en los plazos previstos en el artículo 156.3 por causa imputable al adjudicatario.

c) Haber incumplido las cláusulas que son esenciales en el contrato, incluyendo las condiciones especiales de ejecución establecidas de acuerdo con lo señalado en el artículo 118, cuando dicho incumplimiento hubiese sido definido en los pliegos o en el contrato como infracción grave, concurriendo dolo, culpa o negligencia en el empresario, y siempre que haya dado lugar a la imposición de penalidades o a la indemnización de daños y perjuicios.

d) Haber dado lugar, por causa de la que hubiesen sido declarados culpables, a la resolución firme de cualquier contrato celebrado con una entidad de las comprendidas en el artículo 3 de la presente Ley.

3. Las prohibiciones de contratar afectarán también a aquellas empresas de las que, por razón de las personas que las rigen o de otras circunstancias, pueda presumirse que son continuación o que derivan, por transformación, fusión o sucesión, de otras empresas en las que hubiesen concurrido aquéllas.»

Dos. El artículo 61 queda redactado del siguiente modo:

«Artículo 61. *Apreciación de la prohibición de contratar. Competencia y procedimiento.*

1. Las prohibiciones de contratar relativas a las circunstancias contenidas en las letras c), d), f), g) y h) del apartado 1 del artículo anterior, se apreciarán directamente por los órganos de contratación, subsistiendo mientras concurran las circunstancias que en cada caso las determinan.

2. La prohibición de contratar por las causas previstas en las letras a) y b) del apartado 1 del artículo anterior se apreciará directamente por los órganos de contratación, cuando la sentencia o la resolución administrativa se hubiera pronunciado expresamente sobre su alcance y duración, subsistiendo durante el plazo señalado en las mismas.

En el caso de que la sentencia o la resolución administrativa no contengan pronunciamiento sobre el alcance o duración de la prohibición de contratar; en los casos de la letra e) del apartado primero del artículo anterior; y en los supuestos contemplados en el apartado segundo, también del artículo anterior, el alcance y duración de la prohibición deberá determinarse mediante procedimiento instruido al efecto, de conformidad con lo dispuesto en este artículo.

3. La competencia para fijar la duración y alcance de la prohibición de contratar en el caso de las letras a) y b) del apartado 1 del artículo anterior, en los casos en que no figure en la correspondiente sentencia o resolución, y la competencia para la declaración de la prohibición de contratar en el caso de la letra e) del apartado primero del artículo anterior respecto de la obligación de comunicar la información prevista en materia de clasificación y respecto del registro de licitadores y empresas clasificadas, corresponderá al Ministro de Hacienda y Administraciones Públicas previa propuesta de la Junta Consultiva de Contratación Administrativa del Estado, o

a los órganos que resulten competentes en el ámbito de las Comunidades Autónomas en el caso de la letra e) citada.

A efectos de poder dar cumplimiento a lo establecido en el párrafo anterior, el órgano judicial o administrativo del que emane la sentencia o resolución administrativa deberá remitir de oficio testimonio de aquélla o copia de ésta a la Junta Consultiva de Contratación Administrativa del Estado, sin perjuicio de que por parte de éste órgano, de tener conocimiento de su existencia y no habiendo recibido el citado testimonio de la sentencia o copia de la resolución administrativa, pueda solicitarlos al órgano del que emanaron.

En los supuestos previstos en la letra e) del apartado 1 del artículo anterior referido a casos en que se hubiera incurrido en falsedad al efectuar la declaración responsable a que se refiere el artículo 146, y en los supuestos previstos en el apartado segundo del artículo 60, la declaración de la prohibición de contratar corresponderá al órgano de contratación.

4. La competencia para la declaración de la prohibición de contratar en los casos en que la entidad contratante no tenga el carácter de Administración Pública corresponderá al titular del departamento, presidente o director del organismo al que esté adscrita o del que dependa la entidad contratante o al que corresponda su tutela o control. Si la entidad contratante estuviera vinculada a más de una Administración, será competente el órgano correspondiente de la que ostente el control o participación mayoritaria.

5. Cuando conforme a lo señalado en este artículo, sea necesaria una declaración previa sobre la concurrencia de la prohibición, el alcance y duración de ésta se determinarán siguiendo el procedimiento que en las normas de desarrollo de esta Ley se establezca.

6. En los casos en que por sentencia penal firme así se prevea, la duración de la prohibición de contratar será la prevista en la misma. En los casos en los que ésta no haya establecido plazo, esa duración no podrá exceder de cinco años desde la fecha de la condena por sentencia firme.

En el resto de los supuestos, el plazo de duración no podrá exceder de tres años, para cuyo cómputo se estará a lo establecido en el apartado tercero del artículo 61 bis.

7. En el caso de la letra a) del apartado 1 del artículo anterior, el procedimiento, de ser necesario, no podrá iniciarse una vez transcurrido el plazo previsto para la prescripción de la correspondiente pena, y en el caso de la letra b) del apartado 2 del mismo artículo, si hubiesen transcurrido más de tres meses desde que se produjo la adjudicación.

En los restantes supuestos previstos en dicho artículo, el procedimiento para la declaración de la prohibición de contratar no podrá iniciarse si hubiesen transcurrido más de tres años contados a partir de las siguientes fechas:

a) Desde la firmeza de la resolución sancionadora, en el caso de la causa prevista en la letra b) del apartado 1 del artículo anterior;

b) Desde la fecha en que se hubieran facilitado los datos falsos o desde aquella en que hubiera debido comunicarse la correspondiente información, en los casos previstos en la letra e) del apartado 1 del artículo anterior;

c) Desde la fecha en que fuese firme la resolución del contrato, en el caso previsto en la letra d) del apartado 2 del artículo anterior;

d) En los casos previstos en la letra a) del apartado 2 del artículo anterior, desde la fecha en que se hubiese procedido a la adjudicación del contrato, si la causa es la retirada indebida de proposiciones o candidaturas; o desde la fecha en que hubiese debido procederse a la adjudicación, si la prohibición se fundamenta en el incumplimiento de lo establecido en el apartado segundo del artículo 151.

e) Desde que la entidad contratante tuvo conocimiento del incumplimiento de las condiciones especiales de ejecución del contrato en los casos previstos en la letra c) del apartado segundo del artículo 61 bis.»

Tres. Se introduce un artículo 61 bis, con la siguiente redacción:

«Artículo 61 bis. *Efectos de la declaración de la prohibición de contratar.*

1. En los supuestos en que se den las circunstancias establecidas en el apartado segundo del artículo 60 y en la letra e) del apartado primero del mismo artículo en lo referente a haber incurrido en falsedad al efectuar la declaración responsable del artículo 146 o al facilitar otros datos relativos a su capacidad y solvencia, la prohibición de contratar afectará al ámbito del órgano de contratación competente para su declaración.

Dicha prohibición se podrá extender al correspondiente sector público en el que se integre el órgano de contratación. En el caso del sector público estatal, la extensión de efectos corresponderá al Ministro de Hacienda y Administraciones Públicas, previa propuesta de la Junta Consultiva de Contratación Administrativa del Estado.

En los supuestos en que, de conformidad con lo establecido en el primer párrafo del apartado tercero del artículo anterior respecto a la letra e) del apartado primero del artículo 60, la competencia para la declaración de la prohibición de contratar corresponda a los órganos que resulten competentes en el ámbito de las Comunidades Autónomas, la citada prohibición de contratar afectará a todos los órganos de contratación del correspondiente sector público.

Excepcionalmente, y siempre que previamente se hayan extendido al correspondiente sector público territorial, los efectos de las prohibiciones de contratar a las que se refieren los párrafos anteriores se podrán extender al conjunto del sector público. Dicha extensión de efectos a todo el sector público se realizará por el Ministro de Hacienda y Administraciones Públicas, previa propuesta de la Junta Consultiva de Contratación Administrativa del Estado, y a solicitud de la Comunidad Autónoma o Entidad Local correspondiente en los casos en que la prohibición de contratar provenga de tales ámbitos.

En los casos en que la competencia para declarar la prohibición de contratar corresponda al Ministro de Hacienda y Administraciones Públicas, la misma producirá efectos en todo el sector público.

2. Todas las prohibiciones de contratar, salvo aquellas en que se den alguna de las circunstancias previstas en las letras c), d), g) y h) del apartado primero del artículo 60, se inscribirán en el Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público o el equivalente en el ámbito de las Comunidades Autónomas, en función del ámbito de la prohibición de contratar y del órgano que la haya declarado.

Los órganos de contratación del ámbito de las Comunidades Autónomas o de las entidades locales situadas en su territorio notificarán la prohibición de contratar a los Registros de Licitadores de las Comunidades Autónomas correspondientes, o si no existieran, al Registro Oficial de Licitadores y Empresas Clasificadas del Sector Público.

La inscripción de la prohibición de contratar en el Registro de Licitadores correspondiente caducará pasados 3 meses desde que termine su duración, debiendo procederse de oficio a su cancelación en dicho Registro tras el citado plazo.

3. Las prohibiciones de contratar contempladas en las letras a) y b) del apartado primero del artículo 60 producirán efectos desde la fecha en que devinieron firmes la sentencia o la resolución administrativa en los casos en que aquélla o ésta se hubieran pronunciado sobre el alcance y la duración de la prohibición.

En el resto de supuestos, los efectos se producirán desde la fecha de inscripción en el registro correspondiente.

No obstante lo anterior, en los supuestos previstos en las letras a) y b) del apartado primero del artículo 60 en los casos en que los efectos de la prohibición de contratar se produzcan desde la inscripción en el correspondiente registro, podrán adoptarse, en su caso, por parte del órgano competente para resolver el procedimiento de determinación del alcance y duración de la prohibición, de oficio, o a instancia de parte, las medidas provisionales que estime oportunas para asegurar la eficacia de la resolución que pudiera adoptarse.

4. Las prohibiciones de contratar cuya causa fuera la prevista en la letra f) del apartado primero del artículo 60, producirán efectos respecto de las Administraciones Públicas que se establezcan en la resolución sancionadora que las impuso, desde la fecha en que ésta devino firme.»

Cuatro. El apartado 2 del artículo 150 queda redactado de la siguiente manera:

«2. Los criterios que han de servir de base para la adjudicación del contrato se determinarán por el órgano de contratación y se detallarán en el anuncio, en los pliegos de cláusulas administrativas particulares o en el documento descriptivo.

En la determinación de los criterios de adjudicación se dará preponderancia a aquellos que hagan referencia a características del objeto del contrato que puedan valorarse mediante cifras o porcentajes obtenidos a través de la mera aplicación de las fórmulas establecidas en los pliegos. Cuando en una licitación que se siga por un procedimiento abierto o restringido se atribuya a los criterios evaluables de forma automática por aplicación de fórmulas una ponderación inferior a la correspondiente a los criterios cuya cuantificación dependa de un juicio de valor, deberá constituirse un comité que cuente con un mínimo de tres miembros, formado por expertos no integrados en el órgano proponente del contrato y con cualificación apropiada, al que corresponderá realizar la evaluación de las ofertas conforme a estos últimos criterios, o encomendar esta evaluación a un organismo técnico especializado, debidamente identificado en los pliegos.

La evaluación de las ofertas conforme a los criterios cuantificables mediante la mera aplicación de fórmulas se realizará tras efectuar previamente la de aquellos otros criterios en que no concurra esta circunstancia, dejándose constancia documental de ello. Las normas de desarrollo de esta Ley determinarán los supuestos y condiciones en que deba hacerse pública tal evaluación previa, así como la forma en que deberán presentarse las proposiciones para hacer posible esta valoración separada.

Cuando en los contratos de concesión de obra pública o gestión de servicios públicos se prevea la posibilidad de que se efectúen aportaciones públicas a la construcción o explotación así como cualquier tipo de garantías, avales u otro tipo de ayudas a la empresa, en todo caso figurará como un criterio de adjudicación evaluable de forma automática la cuantía de la reducción que oferten los licitadores sobre las aportaciones previstas en el expediente de contratación.»

Cinco. El artículo 254 queda redactado de la siguiente manera:

«Artículo 254. *Aportaciones públicas a la construcción y garantías a la financiación.*

1. Las Administraciones Públicas podrán contribuir a la financiación de la obra mediante aportaciones que serán realizadas durante la fase de ejecución de las obras, tal como dispone el artículo 240 de esta Ley, o una vez concluidas éstas, y cuyo importe será fijado por los licitadores en sus ofertas dentro de la cuantía máxima que establezcan los pliegos de condiciones.

2. Las aportaciones públicas a que se refiere el apartado anterior podrán consistir en aportaciones no dinerarias del órgano de contratación o de cualquier otra Administración con la que exista convenio al efecto, de acuerdo con la valoración de las mismas que se contenga en el pliego de cláusulas administrativas particulares.

Los bienes inmuebles que se entreguen al concesionario se integrarán en el patrimonio afecto a la concesión, destinándose al uso previsto en el proyecto de la obra, y revertirán a la Administración en el momento de su extinción, debiendo respetarse, en todo caso, lo dispuesto en los planes de ordenación urbanística o sectorial que les afecten.

3. Todas las aportaciones públicas han de estar previstas en el pliego de condiciones determinándose su cuantía en el procedimiento de adjudicación y no podrán incrementarse con posterioridad a la adjudicación del contrato.

4. El mismo régimen establecido para las aportaciones será aplicable a cualquier tipo de garantía, avales y otras medidas de apoyo a la financiación del concesionario que, en todo caso, tendrán que estar previstas en los pliegos.»

Seis. El artículo 256 queda redactado de la siguiente manera:

«Artículo 256. *Aportaciones públicas a la explotación.*

Las Administraciones Públicas podrán otorgar al concesionario las siguientes aportaciones a fin de garantizar la viabilidad económica de la explotación de la obra, que, en todo caso, tendrán que estar previstas en el pliego de condiciones y no podrán incrementarse con posterioridad a la adjudicación del contrato, sin perjuicio del reequilibrio previsto en el artículo 258:

a) Subvenciones, anticipos reintegrables, préstamos participativos, subordinados o de otra naturaleza, para ser aportados desde el inicio de la explotación de la obra o en el transcurso de la misma. La devolución de los préstamos y el pago de los intereses devengados en su caso por los mismos se ajustarán a los términos previstos en la concesión.

b) Ayudas, incluyendo todo tipo de garantías, en los casos excepcionales en que, por razones de interés público, resulte aconsejable la promoción de la utilización de la obra pública antes de que su explotación alcance el umbral mínimo de rentabilidad.»

Siete. El artículo 261 queda redactado de la siguiente manera:

«Artículo 261. *Objeto de la hipoteca de la concesión y pignoración de derechos.*

1. Las concesiones de obras públicas con los bienes y derechos que lleven incorporados serán hipotecables conforme a lo dispuesto en la legislación hipotecaria, previa autorización del órgano de contratación.

No se admitirá la hipoteca de concesiones de obras públicas en garantía de deudas que no guarden relación con la concesión correspondiente.

2. Las solicitudes referentes a las autorizaciones administrativas previstas en este artículo y en el siguiente se resolverán por el órgano competente en el plazo de un mes, debiendo entenderse desestimadas si no resuelve y notifica en ese plazo.

3. Los derechos derivados de la resolución de un contrato de concesión de obra o de gestión de servicio público, a que se refieren los primeros apartados de los artículos 271 y 288, así como los derivados de las aportaciones públicas y de la ejecución de garantías establecidos en los artículos 254 y 256, sólo podrán pignorarse en garantía de deudas que guarden relación con la concesión o el contrato, previa autorización del órgano de contratación, que deberá publicarse en el “Boletín Oficial del Estado” o en los diarios oficiales autonómicos o provinciales.»

Ocho. Los apartados 1 y 3 del artículo 271 quedan redactados de la siguiente manera:

«1. En los supuestos de resolución por causa imputable a la Administración, esta abonará en todo caso al concesionario el importe de las inversiones realizadas por razón de la expropiación de terrenos, ejecución de obras de construcción y adquisición de bienes que sean necesarios para la explotación de la obra objeto de la concesión, atendiendo a su grado de amortización. Al efecto, se aplicará un criterio de amortización lineal. La cantidad resultante se fijará dentro del plazo de seis meses, salvo que se estableciera otro en el pliego de cláusulas administrativas particulares.

En los casos en que la resolución se produzca por causas no imputables a la Administración, el importe a abonar a éste por razón de la expropiación de terrenos, ejecución de obras y adquisición de bienes que deban revertir a la Administración será el que resulte de la valoración de la concesión, determinado conforme a lo dispuesto en el artículo 271 bis.

En todo caso, se entenderá que la resolución de la concesión no es imputable a la Administración cuando obedezca a alguna de las causas previstas en las letras a), b), c), e) y j) del artículo 269 de esta Ley.»

«3. En los supuestos de los párrafos g), h) e i) del artículo 269, y sin perjuicio de lo dispuesto en el apartado 1 de este artículo, la Administración concedente

indemnizará al concesionario por los daños y perjuicios que se le irroguen. Para determinar la cuantía de la indemnización se tendrán en cuenta:

a) los beneficios futuros que el concesionario dejará de percibir, cuantificándolos en la media aritmética de los beneficios antes de impuestos obtenidos durante un período de tiempo equivalente a los años que restan hasta la terminación de la concesión. En caso de que el tiempo restante fuese superior al transcurrido, se tomará como referencia este último.

La tasa de descuento aplicable será la que resulte del coste de capital medio ponderado correspondiente a las últimas cuentas anuales del concesionario.

b) la pérdida del valor de las obras e instalaciones que no hayan de ser entregadas a aquélla, considerando su grado de amortización.»

Nueve. Se añade un nuevo artículo 271 bis con la siguiente redacción:

«Artículo 271 bis. *Nuevo proceso de adjudicación en concesión de obras en los casos en los que la resolución obedezca a causas no imputables a la Administración.*

1. En el supuesto de resolución por causas no imputables a la Administración, el órgano de contratación deberá licitar nuevamente la concesión, siendo el tipo de licitación el que resulte del artículo siguiente. La licitación se realizará mediante subasta al alza siendo el único criterio de adjudicación el precio.

En el caso que quedara desierta la primera licitación, se convocará una nueva licitación en el plazo máximo de un mes, siendo el tipo de licitación el 50 % de la primera.

El adjudicatario de la licitación deberá abonar el importe de ésta en el plazo de dos meses desde que se haya adjudicado la concesión. En el supuesto de que no se abone el citado importe en el indicado plazo, la adjudicación quedará sin efecto, adjudicándose al siguiente licitador por orden o, en el caso de no haber más licitadores, declarando la licitación desierta.

La convocatoria de la licitación podrá realizarse siempre que se haya incoado el expediente de resolución, si bien no podrá adjudicarse hasta que éste no haya concluido. En todo caso, desde la resolución de la concesión a la apertura de las ofertas de la primera licitación no podrá transcurrir un plazo superior a tres meses.

Podrá participar en la licitación todo empresario que haya obtenido la oportuna autorización administrativa en los términos previstos en el apartado 2 del artículo 263.

2. El valor de la concesión, en el supuesto de que la resolución obedezca a causas no imputables a la Administración, será el que resulte de la adjudicación de las licitaciones a las que se refiere el apartado anterior.

En el caso de que la segunda licitación quedara desierta, el valor de la concesión será el tipo de ésta, sin perjuicio de la posibilidad de presentar por el concesionario originario o acreedores titulares al menos de un 5 % del pasivo exigible de la concesionaria, en el plazo máximo de tres meses a contar desde que quedó desierta, un nuevo comprador que abone al menos el citado tipo de licitación, en cuyo caso el valor de la concesión será el importe abonado por el nuevo comprador.

La Administración abonará al primitivo concesionario el valor de la concesión en un plazo de tres meses desde que se haya realizado la adjudicación de la licitación a la que se refiere el apartado anterior o desde que la segunda licitación haya quedado desierta.

En todo caso, el nuevo concesionario se subrogará en la posición del primitivo concesionario quedando obligado a la realización de las actuaciones vinculadas a las subvenciones de capital percibidas cuando no se haya cumplido la finalidad para la que se concedió la subvención.

3. El contrato resultante de la licitación referida en el apartado 1 tendrá en todo caso la naturaleza de contrato de concesión de obra pública, siendo las condiciones del mismo las establecidas en el contrato primitivo que se ha resuelto, incluyendo el plazo de duración.»

Diez. Se añade un nuevo artículo 271 ter con la siguiente redacción:

«Artículo 271 ter. *Determinación del tipo de licitación de la concesión de obras en los casos en los que la resolución obedezca a causas no imputables a la Administración.*

Para la fijación del tipo de la primera licitación, al que se refiere el artículo 271 bis se seguirán las siguientes reglas:

a) El tipo se determinará en función de los flujos futuros de caja que se prevea obtener por la sociedad concesionaria, por la explotación de la concesión, en el periodo que resta desde la resolución del contrato hasta su reversión, actualizados al tipo de descuento del interés de las obligaciones del Tesoro a diez años incrementado en 300 puntos básicos.

Se tomará como referencia para el cálculo de dicho rendimiento medio los últimos datos disponibles publicados por el Banco de España en el Boletín del Mercado de Deuda Pública.

b) El instrumento de deuda que sirve de base al cálculo de la rentabilidad razonable y el diferencial citados podrán ser modificados por la Comisión Delegada del Gobierno para Asuntos Económicos, previo informe de la Oficina Nacional de Evaluación, para adaptarlo a las condiciones de riesgo y rentabilidad observadas en los contratos del sector público.

c) Los flujos netos de caja futuros se cuantificarán en la media aritmética de los flujos de caja obtenidos por la entidad durante un período de tiempo equivalente a los años que restan hasta la terminación. En caso de que el tiempo restante fuese superior al transcurrido, se tomará como referencia este último. No se incorporará ninguna actualización de precios en función de la inflación futura estimada.

d) El valor de los flujos de caja será el que el Plan General de Contabilidad establece en el Estado de Flujos de Efectivo como Flujos de Efectivo de las Actividades de Explotación sin computar en ningún caso los pagos y cobros de intereses, los cobros de dividendos y los cobros o pagos por impuesto sobre beneficios.

e) Si la resolución del contrato se produjera antes de la terminación de la construcción de la infraestructura, el tipo de la licitación será el 70 % del importe equivalente a la inversión ejecutada. A estos efectos se entenderá por inversión ejecutada el importe que figure en las últimas cuentas anuales aprobadas incrementadas en la cantidad resultante de las certificaciones cursadas desde el cierre del ejercicio de las últimas cuentas aprobadas hasta el momento de la resolución. De dicho importe se deducirá el correspondiente a las subvenciones de capital percibidas por el beneficiario, cuya finalidad no se haya cumplido.»

Once. El apartado 1 del artículo 288 queda redactado de la siguiente manera:

«1. En los supuestos de resolución por causa imputable a la Administración, esta abonará al concesionario en todo caso el importe de las inversiones realizadas por razón de la expropiación de terrenos, ejecución de obras de construcción y adquisición de bienes que sean necesarios para la explotación de la obra objeto de la concesión, atendiendo a su grado de amortización. Al efecto, se aplicará un criterio de amortización lineal de la inversión.

Cuando la resolución obedezca a causas no imputables a la Administración, el importe a abonar a éste por razón de la expropiación de terrenos, ejecución de obras y adquisición de bienes que deban revertir a la Administración será el que resulte de la valoración de la concesión, determinado conforme a lo dispuesto en el artículo 271 bis.

En todo caso, se entenderá que no es imputable a la Administración la resolución del contrato cuando ésta obedezca a alguna de las causas establecidas en las letras a) y b) del artículo 223 de esta Ley.»

Doce. Se incorpora una nueva disposición adicional con el siguiente contenido:

«Disposición adicional trigésimo sexta. *La Oficina Nacional de Evaluación.*

1. Se crea la Oficina Nacional de Evaluación que tiene como finalidad analizar la sostenibilidad financiera de los contratos de concesiones de obras y contratos de concesión de servicios públicos.

2. Mediante Orden del Ministro de Hacienda y Administraciones Públicas, previo informe de la Comisión Delegada del Gobierno para Asuntos Económicos, se determinará la composición, organización y funcionamiento de la misma.

3. La Oficina Nacional de Evaluación, con carácter previo a la licitación de los contratos de concesión de obras y de gestión de servicios públicos a celebrar por los poderes adjudicadores dependientes de la Administración General del Estado y de las Corporaciones Locales, evacuará informe preceptivo en los siguientes casos:

a) Cuando se realicen aportaciones públicas a la construcción o a la explotación de la concesión, así como cualquier medida de apoyo a la financiación del concesionario.

b) Las concesiones de obra pública y los contratos de gestión de servicios en las que la tarifa sea asumida total o parcialmente por el poder adjudicador concedente, cuando el importe de las obras o los gastos de primer establecimiento superen un millón de euros.

Asimismo informará de los acuerdos de restablecimiento del equilibrio del contrato, en los casos previstos en los artículos 258.2 y 282.4 del Texto Refundido de la Ley de Contratos del Sector Público, respecto de las concesiones de obras y servicios públicos que hayan sido informadas previamente de conformidad con las letras a) y b) anteriores o que, sin haber sido informadas, supongan la incorporación en el contrato de alguno de los elementos previstos en éstas. Cada Comunidad Autónoma podrá adherirse a la Oficina Nacional de Evaluación para que realice dichos informes o si hubiera creado un órgano u organismo equivalente solicitará estos informes preceptivos al mismo cuando afecte a sus contratos de concesión.

Reglamentariamente se fijarán las directrices apropiadas para asegurar que la elaboración de los informes se realiza con criterios suficientemente homogéneos.

4. Los informes previstos en el apartado anterior evaluarán si la rentabilidad del proyecto obtenida en función del valor de la inversión, las ayudas otorgadas, los flujos de caja esperados y la tasa de descuento establecida es razonable en atención al riesgo de demanda que asuma el concesionario. En dicha evaluación se tendrá en cuenta la mitigación que las ayudas otorgadas puedan suponer sobre otros riesgos distintos del de demanda, que habitualmente deban ser soportados por los operadores económicos.

En los contratos de concesión de obra en los que el abono de la tarifa concesional se realice por el poder adjudicador la oficina evaluará previamente la transferencia del riesgo de demanda al concesionario. Si éste no asume completamente dicho riesgo, el informe evaluará la razonabilidad de la rentabilidad en los términos previstos en el párrafo anterior.

En los acuerdos de restablecimiento del equilibrio del contrato, el informe evaluará si las compensaciones financieras establecidas mantienen una rentabilidad razonable según lo dispuesto en el primer párrafo de este apartado.

5. Los informes serán evacuados, a solicitud del poder adjudicador contratante, en el plazo de treinta días desde la petición o nueva aportación de información al que se refiere el párrafo siguiente. Este plazo podrá reducirse a la mitad siempre que se justifique en la solicitud las razones de urgencia. Estos informes serán publicados a través de la central de información económico-financiera de las Administraciones Públicas dependiente del Ministerio de Hacienda y Administraciones Públicas y estarán disponibles para su consulta por el público a través de medios electrónicos.

El poder adjudicador que formule la petición remitirá la información necesaria a la Oficina, quien evacuará su informe sobre la base de la información recibida. Si dicha Oficina considera que la información remitida no es suficiente, no es completa o requiriere alguna aclaración se dirigirá al poder adjudicador peticionario para que le facilite la información requerida dentro del plazo que ésta señale al efecto. La

información que reciba la Oficina deberá ser tratada respetando los límites que rigen el acceso a la información confidencial.

6. Si la Administración o la entidad destinataria del informe se apartara de las recomendaciones contenidas en un informe preceptivo de la Oficina, deberá motivarlo en un informe que se incorporará al expediente del correspondiente contrato y que será objeto de publicación. En el caso de la Administración General del Estado esta publicación se hará a través de la central de información económico-financiera de las Administraciones Públicas.

7. La Oficina publicará anualmente una memoria de actividad.»

Trece. Se incorpora una nueva disposición transitoria con el siguiente contenido:

«Disposición transitoria décima. *Prohibición de contratar por incumplimiento de la cuota de reserva de puestos de trabajo para personas con discapacidad.*

1. La prohibición de contratar establecida en el artículo 60.1.d) relativa al incumplimiento de la cuota de reserva de puestos de trabajo del 2 por ciento para personas con discapacidad no será efectiva en tanto no se desarrolle reglamentariamente y se establezca qué ha de entenderse por el cumplimiento de dicho requisito a efectos de la prohibición de contratar y cómo se acreditará el mismo, que, en todo caso, será bien mediante certificación del órgano administrativo correspondiente, con vigencia mínima de seis meses, o bien mediante certificación del correspondiente Registro de Licitadores, en los casos en que dicha circunstancia figure inscrita en el mismo.

2. Hasta el momento en que se produzca la aprobación del desarrollo reglamentario a que se refiere el apartado anterior, los órganos de contratación ponderarán en los supuestos que ello sea obligatorio, que los licitadores cumplen lo dispuesto en el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, en relación con la obligación de contar con un dos por ciento de trabajadores con discapacidad o adoptar las medidas alternativas correspondientes, de conformidad con lo dispuesto en la disposición adicional cuarta.»

Disposición final décima. *Modificación de la Ley 17/2012, de 27 de diciembre, de Presupuestos Generales del Estado para el año 2013.*

Se modifica la disposición adicional décima tercera de la Ley 17/2012, de 27 de diciembre, de Presupuestos Generales del Estado para el año 2013, que queda redactada en los siguientes términos:

«Décima tercera. *Subvenciones al transporte marítimo y aéreo para residentes en Canarias, Baleares, Ceuta y Melilla.*

Uno. Con vigencia indefinida tendrán derecho a obtener bonificaciones en las tarifas de los servicios regulares de transporte marítimo y aéreo de pasajeros, los ciudadanos españoles, así como los de los demás Estados miembros de la Unión Europea o de otros Estados firmantes del Acuerdo sobre el Espacio Económico Europeo o de Suiza, sus familiares nacionales de terceros países beneficiarios del derecho de residencia o del derecho de residencia permanente y los ciudadanos nacionales de terceros países residentes de larga duración, que acrediten su condición de residente en las Comunidades Autónomas de Canarias e Illes Balears y en las Ciudades de Ceuta y Melilla.

El derecho de residencia de los familiares de ciudadanos de Estados miembros de la Unión Europea o de otro Estado parte en el Acuerdo del Espacio Económico Europeo se acreditará conforme al Real Decreto 240/2007, de 16 de febrero, sobre entrada, libre circulación y residencia en España de ciudadanos de los Estados miembros de la Unión Europea o de otro Estado parte en el Acuerdo del Espacio Económico Europeo. El derecho de residencia de larga duración de los nacionales de terceros países a que se refiere el párrafo anterior se acreditará conforme a lo

previsto en la Ley Orgánica 4/2000, de 11 de enero, de derechos y libertades de los extranjeros en España y su integración social y su normativa de desarrollo.

Para ciudadanos españoles, de los Estados miembros de la Unión Europea o de los demás Estados firmantes del Acuerdo sobre el Espacio Económico Europeo o Suiza, el documento acreditativo de su identidad será el documento nacional de identidad o pasaporte en vigor. En el caso de los familiares de ciudadanos de Estados miembros de la Unión Europea o de otro Estado parte en el Acuerdo del Espacio Económico Europeo y los ciudadanos nacionales de terceros países residentes de larga duración, su identidad se acreditará mediante la tarjeta española de residencia de familiar de ciudadano de la Unión o de identidad de extranjero en la que debe constar su condición de residente de larga duración, respectivamente. Dichos documentos deben encontrarse en vigor.

En el caso de que telemáticamente se haya constatado que el pasajero cumple las condiciones para ser beneficiario de la subvención, éste podrá acreditar su identidad en el modo aéreo a través de los mismos medios que los pasajeros sin derecho a bonificación. En este caso, el pasajero no tendrá que acreditar su condición de residente ni en facturación ni en embarque.

Dos. El porcentaje de bonificación aplicable en los billetes de transporte marítimo, con vigencia indefinida, para los trayectos directos, ya sean de ida o de ida y vuelta, entre las Comunidades Autónomas de Canarias y las Illes Balears y las Ciudades de Ceuta y Melilla, respectivamente, y el resto del territorio nacional será del 50 por ciento de la tarifa bonificable y en los viajes interinsulares será del 25 por ciento de dicha cuantía.

Tres. El porcentaje de bonificación en las tarifas de los servicios regulares de transporte aéreo de pasajeros, entre las Comunidades Autónomas de Canarias e Illes Balears y las Ciudades de Ceuta y Melilla, respectivamente, y el resto del territorio nacional, así como en los viajes interinsulares será, con vigencia indefinida, del 50 por ciento de la tarifa bonificable por cada trayecto directo de ida o de ida y vuelta.

A estos efectos, se considera trayecto directo de ida aquél que se realiza desde el aeropuerto o helipuerto del punto de origen en los archipiélagos, Ceuta o Melilla, al de destino final, distinto del anterior, en el territorio nacional y viceversa, sin escalas intermedias o con escalas, siempre que estas no superen las 12 horas de duración, salvo aquéllas que vinieran impuestas por las necesidades técnicas del servicio o por razones de fuerza mayor.

A los efectos de esta bonificación, del importe de la tarifa bonificable se deducirá el importe correspondiente a las prestaciones patrimoniales públicas a que se refieren las letras d), e) y f) del artículo 68.2 de la Ley 21/2003, de 7 de julio, de Seguridad Aérea, con independencia de que hayan sido repercutidas o no al pasajero. A tal efecto, dichas prestaciones patrimoniales aparecerán desglosadas en la documentación justificativa de los cupones de vuelo.

Cuatro. La condición de residente en las Comunidades Autónomas de Canarias y las Illes Balears y en las Ciudades de Ceuta y Melilla a los efectos de las bonificaciones reguladas en esta disposición se acreditará mediante el certificado de empadronamiento en vigor.

Reglamentariamente podrán establecerse otros medios para la acreditación de la condición de residente, en sustitución del previsto en este apartado o como adicionales de éste.

Cinco. En relación con la verificación del cumplimiento de los requisitos exigidos en esta disposición:

a) Los órganos gestores de las bonificaciones del Ministerio de Fomento podrán acceder a los servicios de verificación y consulta de datos de identidad, domicilio, residencia, nacionalidad y régimen de extranjería de la Plataforma de Intermediación del Ministerio de Hacienda y Administraciones Públicas con el fin de comprobar el cumplimiento de los requisitos para ser beneficiarios de la subvención y realizar las funciones de control encomendadas a dichos órganos, con las garantías previstas en

la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Ley 58/2003, de 17 de diciembre, General Tributaria.

b) Los órganos gestores podrán facilitar por vía telemática a las agencias, las compañías aéreas o marítimas o sus delegaciones, que comercialicen los títulos de transporte bonificados y lo soliciten, la confirmación del cumplimiento de los requisitos para ser beneficiario de la subvención.

La cesión de datos prevista en los párrafos precedentes y su tratamiento, no requerirá el consentimiento de los interesados ni requerirá informarles sobre dicho tratamiento, de conformidad con lo previsto, respectivamente, en los artículos 11.2, letra a), y 5.5 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

La integración en el sistema telemático de acreditación de la residencia de los sistemas de emisión de billetes y su utilización al emitir billetes subvencionados será obligatoria para todas las compañías, aéreas o marítimas, que emitan billetes aéreos o marítimos subvencionados por razones de residencia en territorios no peninsulares, en todos sus canales de venta.

En el caso de la incorporación a un mercado subvencionado de una nueva compañía de transporte regular aéreo o marítimo, ésta podrá emitir billetes aéreos o marítimos con derecho a subvención, sin necesidad de hacer uso del sistema telemático, durante un máximo de tres meses hasta la implantación efectiva de dicho sistema en todos sus canales de venta.

Seis. Cuando el cumplimiento de los requisitos exigidos para ser beneficiario de estas subvenciones no pueda acreditarse a través de la Plataforma de Intermediación conforme a lo previsto en el apartado Cinco, dichos requisitos se acreditarán por cualquiera de los medios previstos en la normativa de aplicación. A estos efectos, el certificado de empadronamiento se ajustará a lo previsto reglamentariamente en la normativa de desarrollo de estas bonificaciones.

Siete. Sin perjuicio de lo dispuesto en el apartado Uno de esta disposición, las bonificaciones previstas en él para familiares nacionales de terceros países beneficiarios del derecho de residencia o del derecho de residencia permanente y los ciudadanos nacionales de terceros países residentes de larga duración, que acrediten su condición de residente en las Comunidades Autónomas de Canarias e Illes Balears y en las Ciudades de Ceuta y Melilla, surten efectos a partir del 1 de abril de 2013.

Ocho. Además de las obligaciones impuestas por la normativa reguladora de las subvenciones al transporte marítimo y aéreo para residentes en Canarias, Illes Balears, Ceuta y Melilla y para familias numerosas y por la Ley 38/2003, de 17 de noviembre, las compañías aéreas y marítimas, como entidades colaboradoras, deben cumplir lo siguiente:

a) En el caso de las compañías aéreas, presentarán las liquidaciones mensuales de los cupones bonificados volados durante un mes en el transcurso de los dos meses siguientes, salvo autorización expresa de la Dirección General de Aviación Civil por razones excepcionales. Estas liquidaciones podrán contener aquellos cupones volados en los seis meses anteriores que no hayan podido ser incluidos, por causas justificadas, en los ficheros de meses pasados.

En el caso de las compañías marítimas, presentarán las liquidaciones en el transcurso de los dos meses siguientes al periodo reglamentario de liquidación, salvo autorización expresa de la Dirección General de la Marina Mercante por razones excepcionales. Estas liquidaciones podrán contener aquellos embarques bonificados en los seis meses anteriores que no hayan podido ser incluidos, por causas justificadas, en los ficheros de liquidaciones pasadas.

b) En la documentación justificativa de la subvención desglosarán el precio y la identificación de todos los conceptos incluidos en el billete aéreo y marítimo, así como cualquier servicio adicional contratado por el pasajero incluido en el billete.

c) Levantarán un parte de incidente cuando un pasajero que posea un billete subvencionado no acredite su identidad y residencia de conformidad con la

normativa aplicable. Los partes correspondientes a cada periodo de liquidación o, en otro caso, un certificado de inexistencia de incidentes en dicho período serán enviados al órgano gestor durante el periodo siguiente.

d) Cumplir con las obligaciones de registro establecidas reglamentariamente, así como registrar ante el órgano gestor, con anterioridad a su comercialización, las tarifas aéreas que incluyan servicios ajenos al transporte aéreo especificándolo en sus condiciones, así como los convenios, contratos o acuerdos de cualquier tipo, con sus anexos, adendas o modificaciones, susceptibles de generar la emisión de billetes subvencionados, con al menos un mes de antelación a la emisión del primer billete bonificado.

Nueve. Asimismo, las compañías marítimas y aéreas y sus agentes, incluidos los sistemas de reserva, habrán de conservar toda la información y documentación relativa a billetes bonificados tanto por razón de residencia no peninsular como por familias numerosas, cualquiera que sea su forma de almacenamiento, que acredite el importe de la subvención y el cumplimento de los procedimientos recogidos reglamentariamente para la concesión de la subvención, a disposición del Ministerio de Fomento, durante el plazo de prescripción previsto en el artículo 39 de la Ley 38/2003, de 17 de noviembre.

A efectos de la liquidación de las bonificaciones aplicadas, las compañías marítimas, aéreas, y sus agentes, lo que incluye a los sistemas de reserva y a cualquier tercero que haya intervenido en la determinación de la tarifa bonificada, en el pago realizado por el pasajero o en la gestión o aplicación de la bonificación, estarán obligadas a prestar colaboración y facilitar cuanta documentación les sea requerida en relación con las tarifas comercializadas objeto de bonificación, las bonificaciones aplicadas, los pagos realizados por el pasajero y las liquidaciones efectuadas.

La negativa al cumplimiento de esta obligación se considerará resistencia, excusa, obstrucción o negativa a los efectos previstos en el artículo 37 de la Ley 38/2003, de 17 de noviembre, sin perjuicio de las sanciones que, en su caso, pudieran corresponder.

Diez. Se autoriza al órgano gestor a modificar mediante resolución, tras dar trámite de audiencia a las compañías aéreas que exploten los mercados sujetos a subvención y a las principales asociaciones de aerolíneas, el contenido de los modelos de los anexos, en lo que afecta a las bonificaciones al transporte aéreo, del Real Decreto 1316/2001, de 30 de noviembre, por el que se regula la bonificación en las tarifas de los servicios regulares de transporte aéreo y marítimo para los residentes en las Comunidades Autónomas de Canarias y las Illes Balears y en las Ciudades de Ceuta y Melilla.

Once. No serán objeto de liquidación por las compañías marítimas y aéreas, ni de reembolso a éstas:

a) Los billetes subvencionados con tarifas marítimas y aéreas que incluyan respectivamente servicios ajenos al transporte marítimo y aéreo, sean o no repercutidos al pasajero.

b) Los billetes aéreos subvencionados emitidos bajo contratos, convenios o acuerdos de cualquier tipo que no hayan sido registrados y expresamente aprobados por la Dirección General de Aviación Civil.

c) Los conceptos excluidos de bonificación por la normativa de aplicación, entre otros, las ofertas, descuentos, promociones o prácticas comerciales equivalentes, que deben ser aplicados de forma previa al cálculo de la subvención, así como los servicios opcionales del transporte comercializados por la compañía marítima y aérea.

Doce. Verificación de fichero informático de las liquidaciones solicitadas por las compañías marítimas con la relación de los embarques realmente producidos en puertos.

El procedimiento de inspección y control de las bonificaciones al transporte marítimo ha de incluir la comprobación de si los datos de los embarques contenidos

en el fichero informático se corresponden con embarques reales producidos en los puertos. Para ello, las autoridades portuarias remitirán mensualmente a la Dirección General de la Marina Mercante la relación de todos los embarques reales producidos en los puertos correspondientes a los trayectos bonificables.

La relación mensual de todos los embarques reales producidos en cada puerto incluirá las relaciones de embarques de todas y cada una de las escalas que hayan tenido lugar durante ese período. Estas relaciones de embarques de cada trayecto serán recabadas directamente por las autoridades portuarias u organismos competentes en cada caso o, en su defecto, remitidas electrónicamente a éstas por las compañías marítimas. La remisión se realizará en el tiempo y forma que determine la Dirección General de la Marina Mercante, pero en todo caso, deberán haber sido recibidas por el órgano competente antes de que la nave llegue a su destino.

No podrá bonificarse ningún embarque contenido en el fichero informático que no esté incluido en la relación de embarques reales, salvo que se demuestre error u omisión.

Trece. El Gobierno dictará las normas de aplicación y desarrollo de las bonificaciones al transporte, marítimo y aéreo, regular de pasajeros.»

Disposición final undécima. *Modificación de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.*

Se modifica el apartado 2 de la disposición final vigésima primera de la ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras, que queda redactado en los siguientes términos:

«2. No obstante, la disposición transitoria decimotercera y la disposición adicional decimosexta entrarán en vigor el día siguiente al de su publicación. Las disposiciones transitorias cuarta y décima entrarán en vigor el 1 de septiembre de 2015. La disposición final novena entrará en vigor el 1 de julio de 2016. La disposición final duodécima entrará en vigor al día siguiente de la publicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.»

Disposición final duodécima. *Restitución o compensación a los partidos políticos de bienes y derechos incautados en aplicación de la normativa sobre responsabilidades políticas.*

El reconocimiento de los derechos previstos en la Ley 50/2007, de 26 de diciembre, de modificación de la Ley 43/1998, de 15 de diciembre, de restitución o compensación a los partidos políticos de bienes y derechos incautados en aplicación de la normativa sobre responsabilidades políticas del periodo 1936-1939, así como la tramitación y resolución de los procedimientos iniciados al amparo de dicha Ley, seguirán suspendidos hasta que se verifiquen las condiciones que permitan atender las prestaciones que la Ley reconoce sin menoscabo de la financiación de otras actuaciones públicas prioritarias.

Una vez se constate la concurrencia de las expresadas condiciones, el Gobierno aprobará el Reglamento de desarrollo de la Ley, el cual fijará un nuevo plazo para la presentación de las solicitudes de restitución o compensación.

Disposición final decimotercera. *Referencias normativas.*

Las referencias hechas a Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común se entenderán hechas a la Ley del Procedimiento Administrativo Común de las Administraciones Públicas o a la Ley de Régimen Jurídico del Sector Público, según corresponda.

Disposición final decimocuarta. *Título competencial.*

1. Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española que atribuye al Estado competencia exclusiva sobre las bases régimen jurídico de las Administraciones Públicas, así como al amparo de lo previsto en el artículo 149.1.13.ª,

relativo a las bases y coordinación de la planificación general de la actividad económica, y del artículo 149.1.14.ª, relativo a la Hacienda Pública general.

2. No tiene carácter básico y se aplica exclusivamente a la Administración General del Estado y al sector público estatal lo previsto en:

a) La subsección 2.ª referida a los órganos colegiados de la Administración General del Estado de la sección 3.ª del capítulo II del Título preliminar.

b) El Título I relativo a la Administración General del Estado.

c) Lo dispuesto en el Capítulo II relativo a la organización y funcionamiento del sector público institucional estatal, el Capítulo III de los organismos públicos estatales, el Capítulo IV de las Autoridades administrativas independientes, el Capítulo V de las sociedades mercantiles estatales, en el artículo 123.2 del Capítulo VI relativo a los Consorcios, los artículos 128, 130, 131, 132, 133, 135 y 136 del Capítulo VII de las fundaciones del sector público estatal y el Capítulo VIII de los fondos carentes de personalidad jurídica, todos ellos del Título II relativo a la organización y funcionamiento del sector público institucional.

d) Lo previsto en las disposiciones adicionales: cuarta, sobre adaptación de entidades y organismos estatales, quinta, sobre gestión compartida de servicios comunes en organismos públicos estatales, sexta, sobre medios propios, séptima, sobre el registro electrónico estatal de órganos e instrumentos de cooperación, undécima, sobre conflictos de atribuciones intraministeriales, duodécima, sobre Autoridades Portuarias y Puertos del Estado, decimotercera, relativa a las entidades de la Seguridad Social, decimocuarta, sobre la organización militar, decimoquinta, relativa al personal militar, la decimosexta, sobre Servicios territoriales integrados en las Delegaciones del Gobierno, decimoséptima, relativa a la Agencia Estatal de la Administración Tributaria, la decimoctava relativa al Centro Nacional de Inteligencia, la decimonovena relativa al Banco de España y la vigésima relativa al Fondo de Reestructuración Ordenada Bancaria.

Disposición final decimoquinta. *Desarrollo normativo de la Ley.*

Se faculta al Consejo de Ministros y a los Ministros de Presidencia y de Hacienda y Administraciones Públicas, en el ámbito de sus competencias, para dictar cuantas disposiciones reglamentarias sean necesarias para el desarrollo de la presente Ley, así como para acordar las medidas necesarias para garantizar la efectiva ejecución e implantación de las previsiones de esta Ley.

En el plazo de tres meses desde la entrada en vigor de esta Ley, mediante Orden del Ministro de Hacienda y Administraciones Públicas, se desarrollará lo previsto en el artículo 85 sobre la supervisión continua.

Disposición final decimosexta. *Precedencias en actos oficiales.*

Por Real Decreto del Consejo de Ministros, a propuesta del Presidente del Gobierno, se determinarán las precedencias de los titulares de los poderes constitucionales y de las instituciones nacionales, así como las de los titulares de los departamentos ministeriales y de los órganos internos de estos en relación con los actos oficiales.

Disposición final decimoséptima. *Adaptación normativa.*

1. En el plazo de un año a partir de la entrada en vigor de la Ley, se deberán adecuar a la misma las normas estatales o autonómicas que sean incompatibles con lo previsto en esta Ley.

2. Los consorcios creados por una ley singular aprobada por las Cortes Generales con anterioridad a la aprobación de esta Ley seguirán rigiéndose por su legislación especial hasta que se produzca la citada adaptación normativa.

Disposición final decimoctava. *Entrada en vigor.*

1. La presente Ley entrará en vigor al año de su publicación en el «Boletín Oficial del Estado», a excepción del punto cuatro de la disposición final quinta, de modificación de la Ley 22/2003, de 9 de julio, Concursal, de los puntos uno a once de la disposición final novena, de modificación del Texto Refundido de la Ley de Contratos del Sector Público,

aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre y la disposición final decimosegunda, de restitución o compensación a los partidos políticos de bienes y derechos incautados en aplicación de la normativa sobre responsabilidades políticas que entrarán en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado», y el punto doce de la misma disposición final novena, que lo hará a los seis meses de la citada publicación en el «Boletín Oficial del Estado».

2. No obstante, entrarán en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado» la disposición final primera, de modificación de la Ley 23/1982, de 16 de junio, reguladora del Patrimonio Nacional, la disposición final segunda, de modificación del Real Decreto-Ley 12/1995, de 28 de diciembre, sobre medidas urgentes en materia presupuestaria, tributaria y financiera, los puntos uno a tres de la disposición final quinta, de modificación de la Ley 22/2003, de 9 de julio, Concursal, la disposición final séptima, de modificación de la Ley 38/2003, de 17 de noviembre, General de Subvenciones y la disposición final undécima, de modificación de la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

3. La disposición final décima de modificación de la disposición adicional décima tercera de la Ley 17/2012, de 27 de diciembre, de Presupuestos Generales del Estado para el año 2013, entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de que los apartados Uno, primer y segundo párrafo; Dos; Tres, párrafos primero y segundo; Cuatro; Cinco, párrafos primero a cuarto y, Seis, surtirán efectos a partir del 1 de enero de 2013, y de lo dispuesto en el apartado Siete.

§ 4

Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 77, de 31 de marzo de 2021
Última modificación: 12 de julio de 2022
Referencia: BOE-A-2021-5032

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, consagran el derecho de las personas a relacionarse por medios electrónicos con las administraciones públicas, simplificando el acceso a los mismos, y refuerzan el empleo de las tecnologías de la información y las comunicaciones (TIC) en las administraciones públicas, tanto para mejorar la eficiencia de su gestión como para potenciar y favorecer las relaciones de colaboración y cooperación entre ellas.

Ambas leyes recogen los elementos que conforman el marco jurídico para el funcionamiento electrónico de las Administraciones Públicas introduciendo un nuevo paradigma que supera la concepción que inspiró la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su desarrollo reglamentario parcial en la Administración General del Estado y sus organismos públicos vinculados o dependientes a través del Real Decreto 1671/2009, de 6 de noviembre, según la cual la tramitación electrónica no era sino una forma de gestión de los procedimientos.

En este sentido, la Ley 11/2007, de 22 de junio, respondiendo a las nuevas realidades, exigencias y experiencias que se habían puesto de manifiesto, al propio desarrollo de la sociedad de la información y al cambio de circunstancias tecnológicas y sociales, entre otros factores, reconocía el derecho de la ciudadanía a relacionarse electrónicamente con las Administraciones Públicas, y no solo la posibilidad como se preveía en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. La Ley 11/2007, de 22 de junio admitía incluso que, por vía reglamentaria, se estableciese la obligatoriedad de comunicarse con las Administraciones Públicas por medios electrónicos cuando las personas interesadas fuesen personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tuviesen garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

En este contexto, la Ley 39/2015, de 1 de octubre, y la Ley 40/2015, de 1 de octubre, han dado respuesta a la demanda actual en el sentido de que la tramitación electrónica de los procedimientos debe constituir la actuación habitual de las Administraciones Públicas, y no solamente ser una forma especial de gestión de los mismos. En consecuencia, se prevé que las relaciones de las Administraciones entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes se realizará a través de medios electrónicos, y se

establece la obligatoriedad de relacionarse electrónicamente con la Administración para las personas jurídicas, entes sin personalidad y, en algunos supuestos, para las personas físicas, y ello sin perjuicio de la posibilidad de extender esta obligación a otros colectivos, por vía reglamentaria.

Con estos antecedentes, era necesario desarrollar y concretar las previsiones legales con el fin, entre otros aspectos, de facilitar a los agentes involucrados en el uso de medios tecnológicos su utilización efectiva, aclarando y precisando, al mismo tiempo, aquellas materias reguladas en estas leyes que permiten un margen de actuación reglamentaria.

La satisfacción del interesado, por tanto, en el uso de los servicios públicos digitales es fundamental para garantizar adecuadamente sus derechos y el cumplimiento de sus obligaciones en su relación con las Administraciones Públicas. Por ello, es prioritario disponer de servicios digitales fácilmente utilizables y accesibles, de modo que se pueda conseguir que la relación del interesado con la Administración a través del canal electrónico sea fácil, intuitiva, efectiva, eficiente y no discriminatoria.

Por otra parte, a lo largo de las dos últimas décadas, los sucesivos Gobiernos de España han ido adoptando programas para el avance digital alineados con las agendas digitales europeas, en todos los cuales ha estado presente el eje de mejora de la Administración electrónica. Fruto de estos programas, España cuenta con una posición muy favorable para abordar la siguiente fase del proceso de Transformación digital de nuestro país y, en lo que concierne a la Administración electrónica, está situada entre los países más avanzados de la Unión Europea, lo que se ha logrado gracias al esfuerzo continuado de las Administraciones Públicas en la adaptación de sus servicios electrónicos para ofrecer cada vez mejores servicios, más adaptados a las demandas de la ciudadanía y las empresas, y más eficientes. En este esfuerzo, la estrategia de España se ha basado en el impulso de los fundamentos que permiten una tramitación electrónica completa, y en el desarrollo de servicios que pueden ser utilizados libremente por todas las Administraciones Públicas, y que están alineados con los esquemas de interoperabilidad europeos.

Los cambios que se están produciendo con la maduración de tecnologías disruptivas y su aplicación a la gestión de la información y la ejecución de políticas públicas, los nuevos modelos de relación de la ciudadanía y empresas con las Administraciones y la reutilización eficiente de la información son grandes desafíos que para ser afrontados con éxito y para que coadyuven a la Transformación digital exigen como presupuesto contar con un marco regulatorio adecuado, tanto con rango de ley como con rango reglamentario, que garantizando la seguridad jurídica para todos los intervinientes sirva a los objetivos de mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada, incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica y garantizar servicios digitales fácilmente utilizables.

En este sentido, la Agenda España Digital 2025 contiene un eje estratégico específico sobre la Transformación Digital del Sector Público, cuya plasmación se concreta en el cumplimiento de un conjunto de medidas entre las que se encuentra la mejora del marco regulatorio de la Administración digital y específicamente en la aprobación de este real decreto. Por su parte, el Plan de Recuperación, Transformación y Resiliencia (España Puede) incluye entre sus diez políticas palanca de reforma estructural para un crecimiento sostenible e inclusivo, lograr una Administración modernizada a través de su digitalización, tanto a nivel transversal como en ámbitos estratégicos, que actúe como tractor de los cambios tecnológicos. El último hito en estrategia transformadora lo constituye el Plan de Digitalización de las Administraciones Públicas 2021 -2025, que supone un salto decisivo en la mejora de la eficacia y eficiencia de la Administración Pública, en la transparencia y eliminación de trabas administrativas a través de la automatización de la gestión, en una mayor orientación a la personalización de servicios y a la experiencia de usuario, actuando todo ello de elemento catalizador de la innovación tecnológica de nuestro país desde el ámbito público.

En definitiva, el Reglamento que aprueba este real decreto persigue los cuatro grandes objetivos mencionados: mejorar la eficiencia administrativa, incrementar la transparencia y la participación, garantizar servicios digitales fácilmente utilizables y mejorar la seguridad jurídica.

En primer lugar, persigue mejorar la eficiencia administrativa para hacer efectiva una Administración totalmente electrónica e interconectada. Así, se desarrolla y concreta el empleo de los medios electrónicos establecidos en las leyes 39/2015, de 1 de octubre, y 40/2015, de 1 de octubre, para garantizar, por una parte, que los procedimientos administrativos se tramiten electrónicamente por la Administración y, por otra, que la ciudadanía se relacione con ella por estos medios en los supuestos en que sea establecido con carácter obligatorio o aquellos lo decidan voluntariamente.

Un segundo objetivo consiste en incrementar la transparencia de la actuación administrativa y la participación de las personas en la Administración Electrónica. Así, se desarrolla el funcionamiento del Punto de Acceso General electrónico (PAGe), y la Carpeta ciudadana en el Sector Público Estatal. Se regula el contenido y los servicios mínimos a prestar por las sedes electrónicas y sedes electrónicas asociadas y el funcionamiento de los registros electrónicos.

En tercer lugar, el Reglamento persigue garantizar servicios digitales fácilmente utilizables de modo que se pueda conseguir que la relación del interesado con la Administración sea fácil, intuitiva y efectiva cuando use el canal electrónico.

Por último, busca mejorar la seguridad jurídica. Así, se elimina la superposición de regímenes jurídicos distintos, se adapta e integra en el Reglamento que aprueba este real decreto la regulación que aún permanecía vigente del Real Decreto 1671/2009, de 6 de noviembre, procediendo, por ello, a su derogación definitiva y se adecua la regulación al nuevo marco de la Ley 39/2015, de 1 de octubre y la Ley 40/2015, de 1 de octubre.

El real decreto consta de un artículo único que aprueba el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, dos disposiciones transitorias, una disposición derogatoria y cinco disposiciones finales.

Entre las cinco disposiciones finales hay dos que modifican normas vigentes y las tres restantes regulan el título competencial, la habilitación reglamentaria para el desarrollo y ejecución del real decreto y la entrada en vigor. Respecto de las disposiciones modificativas, estas afectan al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y al Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Así, en primer lugar, con relación al Real Decreto 4/2010, de 8 de enero, su artículo 29 establece que el Esquema Nacional de Interoperabilidad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Por ello, la rápida evolución de las tecnologías, la experiencia derivada de la aplicación del Esquema Nacional de Interoperabilidad desde su aprobación hace 10 años, las previsiones de la Ley 39/2015, de 1 de octubre, y de la Ley 40/2015, de 1 de octubre, relativas a la interoperabilidad entre las Administraciones Públicas y sus órganos, organismos públicos y entidades de derecho público vinculados o dependientes, más la necesidad de adecuarse a lo previsto en el Reglamento n.º 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea, por el que se modifican las Directivas 89/686/CEE y 93/15/CEE del Consejo y las Directivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE y 2009/105/CE del Parlamento Europeo y del Consejo y por el que se deroga la Decisión 87/95/CEE del Consejo y la Decisión no 1673/2006/CE del Parlamento Europeo y del Consejo, determinan la necesidad de proceder a modificar ciertos aspectos de su redacción actual. En consecuencia, se modifican los artículos, 9, 11, 14, 16, 17, y 18, así como la disposición adicional primera y el anexo de glosario, a la vez que se suprimen el artículo 19 y las disposiciones adicionales tercera y cuarta.

En segundo lugar, se modifica el Real Decreto 931/2017, de 27 de octubre, para incorporar en la Memoria del Análisis de Impacto Normativo el análisis de la incidencia en los gastos en medios o servicios de la Administración digital dentro del impacto presupuestario de los proyectos y, por otra parte, para incluir dentro del apartado de «Otros impactos» el que tendrá para las personas destinatarias de la norma y para la organización y funcionamiento de la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la aplicación de la normativa proyectada.

Por su parte, el Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos que aprueba el real decreto consta de 65 artículos distribuidos en cuatro títulos, diez disposiciones adicionales y un anexo de definiciones.

El título preliminar del Reglamento comprende las disposiciones generales regulando el objeto y ámbito de aplicación de la norma (que se remite al ámbito del artículo 2 tanto de la Ley 39/2015, de 1 de octubre, como de la Ley 40/2015, de 1 de octubre) y los principios generales que debe respetar el sector público en sus actuaciones y relaciones electrónicas. Entre estos principios se incluyen el de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado; el principio de accesibilidad, para promover que el diseño de los servicios electrónicos garantice la igualdad y no discriminación en el acceso de las personas usuarias, en particular, de las personas discapacitadas y de las personas mayores; el principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias para minimizar el grado de conocimiento tecnológico necesario para el uso del servicio, el principio de interoperabilidad, entendido como la capacidad de los sistemas de información y,por ende, de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos; el principio de proporcionalidad, para que las medidas de seguridad y garantías que se exijan sean adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos y, por último, el principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Asimismo el título preliminar regula el derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas, en aplicación del artículo 14 de la Ley 39/2015, de 1 de octubre, y los canales a través de los cuales las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito.

El título I regula los portales de internet, el PAGe, las sedes electrónicas y sedes electrónicas asociadas (características, creación y supresión, contenido y servicios, y responsabilidad) y el área personalizada a través de la cual cada interesado podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente, que en el ámbito estatal se denomina «Carpeta Ciudadana».

El título II se subdivide en tres capítulos y regula el procedimiento administrativo por medios electrónicos. Así, el capítulo I, sobre «Disposiciones generales» aborda la tramitación administrativa automatizada y el régimen de subsanaciones. Por su parte el capítulo II regula la identificación y autenticación de las Administraciones Públicas y de las personas interesadas y se subdivide en cuatro Secciones: la 1ª aborda las disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad (incluyendo la plataforma de verificación de certificados electrónicos y otros sistemas de identificación), la 2.ª regula la «Identificación electrónica de las Administraciones Públicas y la autenticación del ejercicio de su competencia», que comprende la identificación de las sedes electrónicas y sedes asociadas, la identificación mediante sello electrónico basado en certificado electrónico cualificado, los sistemas de firma electrónica para la actuación administrativa automatizada, la identificación y firma del personal al servicio de las Administraciones Públicas (incluidos los certificados de empleado público con número de identificación profesional) y la autenticación e identificación de las Administraciones emisoras y receptoras en intercambio de datos a través de entornos cerrados de comunicación. La sección 3ª desarrolla la regulación de la identificación y firma de las personas interesadas y, por último, la sección 4ª regula la acreditación de la representación de las personas interesadas (regulando, entre otros extremos, el registro electrónico de apoderamientos).

El título II se cierra con el capítulo III, que en sus dos secciones regula los Registros electrónicos, las notificaciones electrónicas y los otros actos de comunicación electrónicos.

Así, la sección 1ª regula los registros electrónicos (entre otros aspectos, el Registro Electrónico General de cada Administración y la presentación y tratamiento de documentos en registro o las competencias de las Oficinas de asistencia en materia de registros de la Administración General del Estado) y la sección 2ª regula las comunicaciones administrativas a las personas interesadas por medios electrónicos (actos de comunicación electrónica a las personas interesadas distintos de las notificaciones o publicaciones) y las notificaciones electrónicas (incluyendo las reglas generales de la práctica de las notificaciones electrónicas, el aviso de puesta a disposición de la notificación, la notificación a través de la Dirección Electrónica Habilitada única (DEHu) y la notificación electrónica en sede electrónica o sede electrónica asociada).

El título III regula el expediente electrónico y se divide en dos capítulos. El capítulo I regula el documento administrativo electrónico y los requisitos y la emisión de copias auténticas de documentos públicos administrativos o documentos privados, que sean originales o copias auténticas de originales; la formación del expediente administrativo electrónico y el ejercicio de acceso al mismo y a la obtención de copias y la destrucción de documentos. Por su parte, el capítulo II regula la conservación de documentos electrónicos y la definición de archivo electrónico único.

Por último, el título IV se divide en dos capítulos y regula las relaciones y colaboración entre Administraciones Públicas para el funcionamiento electrónico del sector público. Así, el capítulo I aborda la colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos e incluye las obligadas relaciones interadministrativas e interorgánicas por medios electrónicos en el ejercicio de sus competencias, las comunicaciones en la Administración General del Estado, la posibilidad de adhesión a sedes electrónicas y sedes electrónicas asociadas y la regulación del Sistema de Interconexión de Registros (SIR), a través del cual deberán realizarse las interconexiones entre Registros de las Administraciones Públicas, que deberán ser interoperables entre sí y, en el caso de la Administración General del Estado, lo que supone una novedad, también con los sistemas de gestión de expedientes.

El capítulo I del título IV regula también las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015 de 1 de octubre, las plataformas de intermediación de datos (con mención especial a la de ámbito estatal), la remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico completo y, por último, las previsiones el intercambio automático de datos o documentos a nivel europeo previstos en el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012.

El título IV finaliza con el capítulo II, que regula la transferencia y uso compartido de tecnologías entre Administraciones Públicas, abordando, por una parte, la reutilización de sistemas y aplicaciones de las Administraciones Públicas y, por otra, la adhesión a las plataformas, registros o servicios electrónicos de la Administración General del Estado

La parte final del Reglamento consta de diez disposiciones adicionales y un anexo de definiciones. Las primeras regulan la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado; la promoción de la formación del personal al servicio de la Administración General del Estado para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública; la creación del nodo de interoperabilidad para la identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre Estados miembros de la Unión Europea; la adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado, en el ejercicio de potestades administrativas, a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables; la adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado; la situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a

la entrada en vigor de este real decreto; la interoperabilidad de los registros electrónicos de apoderamientos; supletoriedad en Registro Civil; la autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre y, por último, las especialidades por razón de materia.

El Reglamento concluye con un Anexo terminológico que retoma la buena praxis que incluía la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, en una materia de especial complejidad por la imbricación de categorías jurídicas y conceptos tecnológicos en permanente evolución.

El real decreto se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia), en tanto que persigue un interés general al concretar determinados aspectos de la Ley 39/2015, de 1 de octubre y de la Ley 40/2015, de 1 de octubre, que van a facilitar el uso efectivo de los medios electrónicos de la Administración, y el desarrollo necesario de las citadas leyes. La norma es acorde con el principio de proporcionalidad al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento jurídico, estableciéndose un marco normativo estable, integrado y claro. Asimismo, durante el procedimiento de elaboración de la norma, se han formalizado los trámites de consulta pública previa e información pública, que establece la Ley en cumplimiento del principio de transparencia, quedando además justificados en el preámbulo los objetivos que persigue este real decreto. Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación, en materia de cargas administrativas, respecto de las leyes que con esta norma se desarrollan.

Asimismo, el proyecto ha sido informado por la Agencia Española de Protección de Datos y se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y a informe de los diferentes ministerios.

El real decreto se dicta en ejercicio de la habilitación normativa contenida en la disposición final sexta de la Ley 39/2015, de 1 de octubre, y en la disposición final decimoquinta de la Ley 40/2015, de 1 de octubre, para llevar a cabo su desarrollo reglamentario en lo referido a la gestión electrónica de los procedimientos y el funcionamiento electrónico del sector público y garantizar, así, la efectiva aplicación e implantación de las previsiones que ambas leyes establecen, todo ello al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución. Los artículos 15,16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital y del Ministro de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 30 de marzo de 2021,

DISPONGO:

Artículo único. *Aprobación del Reglamento de actuación y funcionamiento del sector público por medios electrónicos.*

Se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Destrucción de documentos en soporte no electrónico.*

(Anulada)

Disposición transitoria segunda. *Portales de internet existentes y aplicaciones específicas en el ámbito estatal.*

1. La supresión de los portales de internet creados en el ámbito estatal antes de la entrada en vigor de este real decreto se regirá por las reglas aplicables en el momento de su creación.

2. En el plazo de seis meses desde la entrada en vigor de este real decreto, en el ámbito de cada ministerio se analizará la oportunidad del mantenimiento de sus portales de internet existentes y los de sus organismos públicos o entidades de derecho público vinculados o dependientes respectivos, así como de las páginas web promocionales («microsites»). Para ese análisis se aplicarán los mismos criterios previstos en el artículo 6 para la creación de nuevos portales y se decidirá acerca de su mantenimiento o su supresión.

En caso de que se decida la supresión, se valorará si es pertinente o no incorporar en el PAGe de la Administración General del Estado la información que se ha contenido en dichos portales hasta la supresión.

3. Realizado el proceso previsto en el apartado anterior, en el plazo máximo de un año desde la entrada en vigor de este real decreto se publicará en el PAGe de la Administración General del Estado una Resolución del Secretario General de Función Pública, en la que figurará el listado de portales de internet activos de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes de esta.

4. En el plazo máximo de un año desde la entrada en vigor de este real decreto, y a partir de la información facilitada por los ministerios, la Secretaría General de Administración Digital realizará el censo de aplicaciones específicas diseñadas para dispositivos móviles («app») para su utilización en los procedimientos de la Administración General del Estado.

5. En el ámbito de la Administración General del Estado, los portales de internet muy reconocidos e identificables por los usuarios, creados antes de la entrada en vigor de este real decreto se regirán por las reglas aplicables en el momento de su creación en cuanto a nomenclatura, sin necesidad de que modifiquen el nombre del dominio de segundo nivel.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto y, en concreto, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Disposición final primera. *Títulos competenciales.*

1. Este real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de procedimiento administrativo común y para dictar las bases del régimen jurídico de las Administraciones Públicas.

2. Los artículos 15, 16, 23, 26, 28.2, 28.3 y 29.4 y la disposición adicional tercera del Reglamento que aprueba este real decreto, en cuanto a su relación con la ciberseguridad y su impacto en la seguridad de las redes y sistemas de información se dictan, además, de acuerdo con lo dispuesto en los artículos 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva en materia de telecomunicaciones y en materia de seguridad pública, respectivamente.

3. No tiene carácter básico y será de aplicación únicamente en el ámbito estatal lo dispuesto en:

a) La disposición transitoria segunda y la disposición final tercera de este real decreto.

b) El segundo párrafo del apartado 3 del artículo 3, los artículos 6, 7.4, 8, 10.3, 10.4, 13.2, 17, 18.2, 19.3, 19.4, 21.4, 23.2, 24, 25.4, 28.3, 30.2, 31, 33, 36, 38.1, el segundo párrafo del apartado 4 del artículo 39, los artículos 40, 42.5, 48, 53.5, 55.2, 57, 60.3, 62.2 y las disposiciones adicionales primera, segunda, cuarta, quinta, sexta, el segundo apartado de la disposición adicional séptima del Reglamento que aprueba este real decreto.

Disposición final segunda. *Modificación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.*

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica queda modificado como sigue:

Uno. El artículo 9 queda redactado del siguiente modo:

«Artículo 9. *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.»

Dos. El párrafo a) del artículo 11.3, queda redactado como sigue:

«a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.»

Tres. Se modifica el artículo 14, que queda redactado como sigue:

«Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.»

Cuatro. Se modifica el artículo 16, que queda redactado como sigue:

«Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.

b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.

c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.

d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.

e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.

f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.

b) Permiten conocer su código fuente.

c) Pueden modificarse o mejorarse.

d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.

4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.

b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.»

Cinco. Se modifica el artículo 17, que queda redactado como sigue:

«Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.

2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.

b) Documentación asociada.

c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.

d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.»

Seis. Se modifica el artículo 18, que queda redactado como sigue:

«Artículo 18. *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las

reglas de creación y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.»

Siete. Se elimina el artículo 19.

Ocho. Se modifica la disposición adicional primera, que queda redactada como sigue:

«Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos

administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.»

Nueve. Se suprime la disposición adicional tercera.

Diez. Se suprime la disposición adicional cuarta.

Once. Se modifica el anexo de la forma siguiente:

1. Se suprime el término « Familia».

2. A continuación del término «Índice electrónico» se sustituye el vigente término «Infraestructuras y servicios comunes» por el término «Infraestructura o servicio común» con la siguiente redacción:

«Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.»

3. A continuación del término «Estándar abierto» se introduce el término «Ficheros de implementación de las políticas de firma« con la siguiente redacción:

«Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.»

Disposición final tercera. *Modificación del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo.*

Se modifican el párrafo segundo de la letra d) y la letra g) del apartado 1 del artículo 2 del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, que quedan redactados como sigue:

«2.º El Impacto presupuestario comprenderá, al menos, una referencia a los efectos en los ingresos y gastos públicos e incluirá la incidencia en los gastos de personal, dotaciones o retribuciones, gastos en medios o servicios de la Administración digital o cualesquiera otros gastos al servicio del sector público.»

«g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma.»

Disposición final cuarta. *Habilitación normativa.*

Se faculta a la persona titular del Ministerio de Política Territorial y Función Pública y a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital en el ámbito de sus competencias, para dictar las disposiciones y adoptar las medidas necesarias para el desarrollo y ejecución de este real decreto y del Reglamento que aprueba, así como para modificar el anexo del mismo.

Disposición final quinta. *Entrada en vigor.*

Este real decreto entrará en vigor el día 2 de abril de 2021.

REGLAMENTO DE ACTUACIÓN Y FUNCIONAMIENTO DEL SECTOR PÚBLICO POR MEDIOS ELECTRÓNICOS

TÍTULO PRELIMINAR

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. Este Reglamento tiene por objeto el desarrollo de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en lo referido a la actuación y el funcionamiento electrónico del sector público.

2. El ámbito subjetivo de aplicación es el establecido en el artículo 2 de la Ley 39/2015, de 1 de octubre, y el artículo 2 de la Ley 40/2015, de 1 de octubre.

Artículo 2. *Principios generales.*

El sector público deberá respetar los siguientes principios en sus actuaciones y relaciones electrónicas:

a) Los principios de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías y sistemas de comunicaciones electrónicas, para garantizar tanto la independencia en la elección de las alternativas tecnológicas necesarias para relacionarse

con las Administraciones Públicas por parte de las personas interesadas y por el propio sector público, como la libertad para desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado. A estos efectos, el sector público utilizará estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado.

Las herramientas y dispositivos que deban utilizarse para la comunicación por medios electrónicos, así como sus características técnicas, serán no discriminatorios, estarán disponibles de forma general y serán compatibles con los productos informáticos de uso general.

b) El principio de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

c) El principio de facilidad de uso, que determina que el diseño de los servicios electrónicos esté centrado en las personas usuarias, de forma que se minimice el grado de conocimiento necesario para el uso del servicio.

d) El principio de interoperabilidad, entendido como la capacidad de los sistemas de información y, por ende, de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

e) El principio de proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones electrónicos.

f) El principio de personalización y proactividad, entendido como la capacidad de las Administraciones Públicas para que, partiendo del conocimiento adquirido del usuario final del servicio, proporcione servicios precumplimentados y se anticipe a las posibles necesidades de los mismos.

Artículo 3. *Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas.*

1. Estarán obligados a relacionarse a través de medios electrónicos con las Administraciones Públicas para la realización de cualquier trámite de un procedimiento administrativo, al menos, los sujetos a los que se refiere el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

2. Las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas podrán ejercitar su derecho a relacionarse electrónicamente con la Administración Pública de que se trate al inicio del procedimiento y, a tal efecto, lo comunicarán al órgano competente para la tramitación del mismo de forma que este pueda tener constancia de dicha decisión. La voluntad de relacionarse electrónicamente o, en su caso, de dejar de hacerlo cuando ya se había optado anteriormente por ello, podrá realizarse en una fase posterior del procedimiento, si bien deberá comunicarse a dicho órgano de forma que quede constancia de la misma. En ambos casos, los efectos de la comunicación se producirán a partir del quinto día hábil siguiente a aquel en que el órgano competente para tramitar el procedimiento haya tenido constancia de la misma.

3. De acuerdo con lo previsto en el apartado 3 del artículo 14 de la Ley 39/2015, de 1 de octubre, la obligatoriedad de relacionarse electrónicamente podrá establecerse reglamentariamente por las Administraciones Públicas para determinados procedimientos y para ciertos colectivos de personas físicas que, por razón de su capacidad económica, técnica, dedicación profesional u otros motivos, quede acreditado que tienen acceso y disponibilidad de los medios electrónicos necesarios.

A tal efecto, en el ámbito estatal la mencionada obligatoriedad de relacionarse por medios electrónicos con sus órganos, organismos y entidades de derecho público podrá ser establecida por real decreto acordado en Consejo de Ministros o por orden de la persona titular del Departamento competente respecto de los procedimientos de que se trate que afecten al ámbito competencial de uno o varios Ministerios cuya regulación no requiera de norma con rango de real decreto. Asimismo, se publicará en el Punto de Acceso General electrónico (PAGe) de la Administración General del Estado y en la sede electrónica o sede asociada que corresponda.

Artículo 4. *Canales de asistencia para el acceso a los servicios electrónicos.*

Las Administraciones Públicas prestarán la asistencia necesaria para facilitar el acceso de las personas interesadas a los servicios electrónicos proporcionados en su ámbito competencial a través de alguno o algunos de los siguientes canales:

a) Presencial, a través de las oficinas de asistencia que se determinen.
b) Portales de internet y sedes electrónicas.
c) Redes sociales.
d) Telefónico.
e) Correo electrónico.
f) Cualquier otro canal que pueda establecerse de acuerdo con lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre.

TÍTULO I

Portales de internet, Punto de Acceso General electrónico y sedes electrónicas

Artículo 5. *Portales de internet de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 39 de la Ley 40/2015, de 1 de octubre, se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información y, en su caso, a la sede electrónica o sede electrónica asociada correspondiente.
2. Cada Administración podrá determinar los contenidos y canales mínimos de atención a las personas interesadas y de difusión y prestación de servicios que deban tener sus portales, así como criterios obligatorios de imagen institucional. En cualquier caso, deberán tenerse en cuenta los contenidos, formatos y funcionalidades que en la normativa de reutilización, accesibilidad y transparencia se establezcan como obligatorios para los sitios web.
3. Los portales de internet dispondrán de sistemas que permitan el establecimiento de medidas de seguridad de acuerdo con lo establecido en Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Artículo 6. *Creación y supresión de portales de internet en el ámbito estatal.*

1. En el ámbito estatal, la creación o supresión de portales se llevará a cabo por orden de la persona titular del ministerio correspondiente o por resolución de la persona titular del órgano superior, en el caso de la Administración General del Estado, y por resolución de la persona titular de la Presidencia o de la Dirección en el caso de sus organismos públicos y entidades de derecho público vinculados o dependientes.

La creación requerirá informe favorable de la Comisión Ministerial de Administración Digital respectiva y posterior comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital. Para obtener dicho informe favorable, la propuesta de creación del nuevo portal se deberá justificar en términos de eficiencia en la asignación y utilización de los recursos públicos e interés prioritario para la implantación de una política pública o la aplicación de la normativa de la Unión Europea o nacional y a tal efecto el órgano promotor de la creación del nuevo portal remitirá una memoria justificativa y económica.

La supresión de portales requerirá la previa comunicación al Ministerio de Política Territorial y Función Pública y al Ministerio de Asuntos Económicos y Transformación Digital.

2. El acto o resolución de creación de un nuevo portal previsto en el apartado anterior contendrá, al menos, la identificación de su dirección electrónica, que deberá incluir el nombre de dominio de segundo nivel «.gob.es», su ámbito funcional y, en su caso, orgánico y la finalidad para la que se crea. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado.

3. En el ámbito estatal los portales de internet a los que se refiere este artículo deberán estar referenciados en el PAGe de la Administración General del Estado.

Artículo 7. *Punto de Acceso General electrónico.*

1. Las Administraciones Públicas contarán con un Punto de Acceso General electrónico (PAGe).

2. El PAGe de cada Administración Pública facilitará el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente.

3. El PAGe dispondrá de una sede electrónica, a través de la cual se podrá acceder a todas las sedes electrónicas y sedes asociadas de la Administración Pública correspondiente.

Además, esta sede podrá incluir un área personalizada a través de la cual cada interesado, mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos personales, podrá acceder a su información, al seguimiento de los trámites administrativos que le afecten y a las notificaciones y comunicaciones en el ámbito de la Administración Pública competente.

4. El PAGe de la Administración General del Estado y su sede electrónica serán gestionados por el Ministerio de Política Territorial y Función Pública en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

En dicha sede electrónica está alojada la Dirección Electrónica Habilitada única a la que se refiere el artículo 43 de la Ley 39/2015, de 1 de octubre.

El PAGe de la Administración General del Estado, a través de su sede, permitirá la comprobación de la autenticidad e integridad de los documentos facilitados por el sector público estatal a través del Código Seguro de Verificación o de cualquier otro sistema de firma o sello basado en certificado electrónico cualificado que se haya utilizado en su generación. También permitirá, en su caso, su recuperación.

5. El PAGe de la Administración General del Estado podrá interoperar con portales web oficiales de la Unión Europea.

Artículo 8. *Carpeta Ciudadana del sector público estatal.*

1. La Carpeta Ciudadana es el área personalizada de las personas interesadas a que se refiere el artículo 7.3 en su relación con el sector público estatal. Además del interesado podrán acceder a la Carpeta Ciudadana:

a) Sus representantes legales.

b) Quien ostente un poder general previsto en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre, otorgado por el interesado e inscrito en el Registro Electrónico de Apoderamientos.

2. La Carpeta Ciudadana será accesible a través de la sede electrónica del PAGe de la Administración General del Estado y podrá ofrecer, entre otras, las funcionalidades siguientes para el interesado o sus representantes:

a) Permitir el seguimiento del estado de tramitación de los procedimientos en que sea interesado, de acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/ 2015, de 1 de octubre.

b) Permitir el acceso a sus comunicaciones y notificaciones.

c) Conocer qué datos suyos obran en poder del sector público estatal, sin perjuicio de las limitaciones que establezca la normativa vigente.

d) Facilitar la obtención de certificaciones administrativas exigidas por la normativa correspondiente.

3. El interesado accederá a la Carpeta Ciudadana mediante los sistemas de identificación a los que se refiere el artículo 9.2 de la Ley 39/2015, de 1 de octubre.

4. El interesado deberá asegurar el buen uso de los sistemas de identificación y velar por que el acceso a su carpeta Ciudadana solo se haga por sí mismo o por tercero autorizado.

Artículo 9. *Sedes electrónicas de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, una sede electrónica es aquella dirección electrónica disponible para la ciudadanía por medio de redes de telecomunicaciones. Mediante dicha sede electrónica se realizarán todas las actuaciones y trámites referidos a procedimientos o a servicios que requieran la identificación de la Administración Pública y, en su caso, la identificación o firma electrónica de las personas interesadas.

2. La titularidad de la sede electrónica corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ámbito de sus competencias.

Artículo 10. *Creación y supresión de las sedes electrónicas y sedes electrónicas asociadas.*

1. Se podrán crear una o varias sedes electrónicas asociadas a una sede electrónica atendiendo a razones técnicas y organizativas. La sede electrónica asociada tendrá consideración de sede electrónica a todos los efectos.

2. El acto o resolución de creación o supresión de una sede electrónica o sede electrónica asociada será publicado en el boletín oficial que corresponda en función de cuál sea la Administración Pública titular de la sede o sede asociada y también en el directorio del Punto de Acceso General Electrónico que corresponda. En el caso de las entidades locales, el boletín oficial será el de la provincia al que pertenezca la entidad.

El acto o resolución de creación determinará, al menos:

a) El ámbito de aplicación de la sede electrónica o sede electrónica asociada.

b) La identificación de la dirección electrónica de referencia de la sede electrónica o sede electrónica asociada que se cree, así como de las direcciones electrónicas de las sedes electrónicas que desde el momento de la creación ya sean asociadas de aquella. Las sedes electrónicas asociadas con posterioridad a la publicación del instrumento de creación se referenciarán en la mencionada dirección electrónica.

c) La identificación de su titular.

d) La identificación del órgano u órganos encargados de la gestión y de los servicios puestos a disposición en la misma.

3. En el ámbito estatal, tanto la creación o supresión de una sede electrónica asociada a la sede electrónica del PAGe de la Administración General del Estado como la creación o supresión de sedes electrónicas o sedes electrónicas asociadas de los organismos públicos y entidades de derecho público vinculados o dependientes se hará mediante orden de la persona titular del Departamento competente o por resolución de la persona titular de la Presidencia o de la Dirección del organismo o entidad de derecho público competente, con el informe previo favorable del Ministerio de Política Territorial y Función Pública y del Ministerio de Asuntos Económicos y Transformación Digital.

4. Para obtener los informes previos favorables a que se refiere el apartado anterior, la propuesta de creación de la nueva sede electrónica o, en su caso, sede electrónica asociada se tendrá que justificar, en términos de eficiencia en la asignación y utilización de recursos públicos. A tal efecto, el órgano promotor de la creación de la sede electrónica remitirá una memoria justificativa y económica en que se explicite el volumen de trámites que está previsto gestionar a través de la misma, los efectos presupuestarios y económicos de su establecimiento, su incidencia en la reducción del tiempo de resolución de los procedimientos y de cargas administrativas para las personas interesadas y cualquier otra razón de interés general que justifique su creación.

Artículo 11. *Contenido y servicios de las sedes electrónicas y sedes asociadas.*

1. Toda sede electrónica o sede electrónica asociada dispondrá del siguiente contenido mínimo a disposición de las personas interesadas:

a) La identificación de la sede electrónica o sede electrónica asociada, así como del órgano u organismo titular de la misma y los órganos competentes para la gestión de la información, servicios, procedimientos y trámites puestos a disposición en ella.

b) La identificación del acto o disposición de creación y el acceso al mismo, directamente o mediante enlace a su publicación en el Boletín Oficial correspondiente.

c) La información necesaria para la correcta utilización de la sede electrónica, incluyendo su mapa o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles, así como la relativa a propiedad intelectual, protección de datos personales y accesibilidad.

d) La relación de sistemas de identificación y firma electrónica que sean admitidos o utilizados en la misma.

e) La normativa reguladora del Registro al que se acceda a través de la sede electrónica.

f) La fecha y hora oficial, así como el calendario de días inhábiles a efectos del cómputo de plazos aplicable a la Administración en que se integre el órgano, organismo público o entidad de derecho público vinculado o dependiente que sea titular de la sede electrónica o sede electrónica asociada.

g) Información acerca de cualquier incidencia técnica que acontezca e imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, así como de la ampliación del plazo no vencido que, en su caso, haya acordado el órgano competente debido a dicha circunstancia.

h) Relación actualizada de los servicios, procedimientos y trámites disponibles

i) Relación actualizada de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites descritos en la letra anterior. Cada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje.

2. Las sedes electrónicas y sedes electrónicas asociadas dispondrán, al menos, de los siguientes servicios a disposición de las personas interesadas:

a) Un acceso a los servicios y trámites disponibles en la sede electrónica o sede electrónica asociada, con indicación de los plazos máximos de duración de los procedimientos, excluyendo las posibles ampliaciones o suspensiones que en su caso, pudiera acordar el órgano competente.

b) Un enlace para la formulación de sugerencias y quejas ante los órganos que en cada caso resulten competentes.

c) Los mecanismos de comunicación y procedimiento de reclamación establecidos al respecto de los requisitos de accesibilidad de los sitios web y aplicaciones móviles del sector público.

d) Un sistema de verificación de los certificados de la sede electrónica.

e) Un sistema de verificación de los sellos electrónicos de los órganos, organismos públicos o entidades de derecho público que abarque la sede electrónica o sede electrónica asociada.

f) Un servicio de comprobación de la autenticidad e integridad de los documentos emitidos por los órganos, organismos públicos o entidades de derecho público comprendidos en el ámbito de la sede electrónica, que hayan sido firmados por cualquiera de los sistemas de firma conformes a la Ley 40/2015, 1 de octubre, y para los cuales se haya generado un código seguro de verificación.

g) Un acceso a los modelos, y sistemas de presentación masiva, de uso voluntario, que permitan a las personas interesadas presentar simultáneamente varias solicitudes en la forma que establezca, en su caso, cada Administración, organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

h) El acceso a los modelos normalizados de presentación de solicitudes que establezca, en su caso, cada Administración u organismo público o entidad de derecho público titular de la sede electrónica o sede electrónica asociada.

i) Un servicio de consulta del directorio geográfico de oficinas de asistencia en materia de registros, que permita al interesado identificar la más próxima a su dirección de consulta.

3. De acuerdo con lo previsto en el artículo 66.1 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas deberán mantener y actualizar en la sede electrónica correspondiente un listado con los códigos de identificación vigentes de sus órganos, centros o unidades administrativas.

Artículo 12. *Responsabilidad sobre la sede electrónica o sede electrónica asociada.*

1. El titular de la sede electrónica y, en su caso, de la sede electrónica asociada, será responsable de la integridad, veracidad y actualización de la información y los servicios de su competencia a los que pueda accederse a través de la misma.

2. En caso de que la sede electrónica o sede electrónica asociada contenga un enlace o vínculo a otra sede o sede asociada, será el titular de esta última el responsable de la integridad, veracidad y actualización de la información o procedimientos que figuren en la misma, sin perjuicio de la debida diligencia del titular de la primera respecto de la incorporación de los contenidos en la misma.

3. En caso de que una sede electrónica o sede electrónica asociada contenga procedimientos, servicios o ambos, cuya competencia corresponda a otro órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente, sea de la misma o de diferente Administración, el titular de la competencia será responsable de la integridad, veracidad y actualización de lo relativo a dichos procedimientos, servicios o ambos sin perjuicio de la debida diligencia del titular de la sede electrónica o sede electrónica asociada respecto de la incorporación de los contenidos en la misma.

TÍTULO II

Procedimiento administrativo por medios electrónicos

CAPÍTULO I

Disposiciones generales

Artículo 13. *Actuación administrativa automatizada.*

1. La tramitación electrónica de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada de acuerdo con lo previsto en el artículo 41 de la Ley 40/2015, de 1 de octubre.

2. En el ámbito estatal la determinación de una actuación administrativa como automatizada se autorizará por resolución del titular del órgano administrativo competente por razón de la materia o del órgano ejecutivo competente del organismo o entidad de derecho público, según corresponda, y se publicará en la sede electrónica o sede electrónica asociada. La resolución expresará los recursos que procedan contra la actuación, el órgano administrativo o judicial, en su caso, ante el que hubieran de presentarse y plazo para interponerlos, sin perjuicio de que las personas interesadas puedan ejercitar cualquier otro que estimen oportuno y establecerá medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos de las personas interesadas.

3. En el ámbito de las Entidades Locales, en caso de actuación administrativa automatizada se estará a lo dispuesto en la disposición adicional octava del Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.

Artículo 14. *Régimen de subsanación.*

1. Si existe la obligación del interesado de relacionarse a través de medios electrónicos y aquel no los hubiese utilizado, el órgano administrativo competente en el ámbito de actuación requerirá la correspondiente subsanación, advirtiendo al interesado, o en su caso su representante, que, de no ser atendido el requerimiento en el plazo de diez días, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de la Ley 39/2015, de 1 de octubre.

Este régimen de subsanación será asimismo aplicable a las personas físicas no obligadas a relacionarse a través de medios electrónicos con las Administraciones Públicas que, de acuerdo con lo dispuesto en el artículo 3.2, hayan ejercitado su derecho a relacionarse electrónicamente con la Administración Pública de que se trate.

Cuando se trate de una solicitud de iniciación del interesado, la fecha de la subsanación se considerará a estos efectos como fecha de presentación de la solicitud de acuerdo con el artículo 68.4 de dicha ley.

2. De acuerdo con lo establecido en el artículo 39.1 de este Reglamento, en el caso de que las Administraciones Públicas hayan determinado los formatos y estándares a los que deberán ajustarse los documentos presentados por el interesado, si este incumple dicho requisito se le requerirá para que, en el plazo de diez días, subsane el defecto advertido en los términos establecidos en los artículos 68.1, cuando se trate de una solicitud de iniciación, y 73.2, cuando se trate de otro acto, ambos de la Ley 39/2015, de 1 de octubre, con la indicación de que, si así no lo hiciera y previa resolución que deberá ser dictada en los términos previstos en el artículo 21 de dicha ley, se le tendrá por desistido de su solicitud o se le podrá declarar decaído en su derecho al trámite correspondiente, respectivamente.

3. En el caso de que el escrito o solicitud presentada adolezca de cualquier otro defecto subsanable, por la falta de cumplimiento de los requisitos exigidos en los artículos 66, 67 y 73 de la Ley 39/2015, de 1 de octubre, o por la falta de otros requisitos exigidos por la legislación específica aplicable, se requerirá su subsanación en el plazo de diez días, en los términos de los artículos 68.1 y 73.1 de la citada ley. Este plazo podrá ser ampliado hasta cinco días, a petición del interesado o a iniciativa del órgano, cuando la aportación de los documentos requeridos, en su caso, presente dificultades especiales, siempre que no se trate de procedimientos selectivos o de concurrencia competitiva.

CAPÍTULO II

De la identificación y autenticación de las Administraciones Públicas y las personas interesadas

Sección 1.ª Disposiciones comunes a la identificación y autenticación y condiciones de interoperabilidad

Artículo 15. *Sistemas de identificación, firma y verificación.*

1. Las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la normativa vigente sobre firma electrónica y resulten adecuados para garantizar la identificación de las personas interesadas y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para garantizar el origen e integridad de los documentos electrónicos:

a) Sistemas de identificación de las sedes electrónicas y sedes electrónicas asociadas.

b) Sello electrónico basado en un certificado electrónico cualificado y que reúna los requisitos exigidos por la legislación de firma electrónica.

c) Sistemas de firma electrónica para la actuación administrativa automatizada.

d) Firma electrónica del personal al servicio de las Administraciones Públicas.

e) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

3. Las personas interesadas podrán utilizar los siguientes sistemas de identificación y firma en sus relaciones electrónicas con las Administraciones Públicas:

a) De acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de los sistemas descritos en las letras a), b) y c) de dicho artículo. En este último supuesto los sistemas deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

b) Asimismo, se considerarán válidos a efectos de firma electrónica ante las Administraciones Públicas los sistemas previstos en las letras a), b) y c) del artículo 10.2 de la Ley 39/2015, de 1 de octubre.

c) De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados.

4. La Administración no será responsable de la utilización por terceras personas de los medios de identificación personal y firma electrónica del interesado, salvo que concurran los requisitos establecidos en el artículo 32 de la Ley 40/2015, de 1 de octubre, para la exigencia de responsabilidad patrimonial.

Artículo 16. *Plataformas de verificación de certificados electrónicos y de otros sistemas de identificación.*

1. La Administración General del Estado dispondrá de una plataforma para la verificación de la vigencia y del contenido de los certificados cualificados admitidos en el sector público. El sistema deberá permitir que tal verificación se pueda llevar a cabo de forma libre y gratuita, para el sector público.

La Secretaría General de Administración Digital será el órgano responsable de esta plataforma, que estará disponible para todo el sector público previa formalización del correspondiente instrumento de adhesión.

2. Esta plataforma dispondrá de una declaración de prácticas de validación en la que se detallarán las obligaciones que se comprometen a cumplir tanto la plataforma como las personas usuarias de la misma en relación con los servicios de verificación. Esta declaración estará disponible al público por vía electrónica y con carácter gratuito.

3. Los prestadores cualificados de servicios de confianza deberán facilitar a esta plataforma el acceso electrónico y gratuito para la verificación de la vigencia de los certificados electrónicos emitidos por aquellos en virtud de su cualificación de acuerdo con la legislación aplicable en materia de servicios electrónicos de confianza.

Artículo 17. *Política de firma electrónica y de certificados en el ámbito estatal.*

1. La política de firma electrónica y de certificados en el ámbito estatal, está constituida por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica.

2. Sin perjuicio de las obligaciones de los prestadores de servicios de confianza previstas en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y resto de normativa vigente, la política de firma electrónica y certificados deberá contener en todo caso:

a) La definición de su ámbito de aplicación.

b) Los requisitos de las firmas electrónicas presentadas ante los órganos de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes.

c) Las especificaciones técnicas y operativas para la definición y prestación de los servicios de confianza asociados a las nuevas formas de identificación y autenticación de la Administración General del Estado y de sus organismos públicos y entidades vinculados o dependientes recogidas en este Reglamento.

3. La política de firma electrónica y certificados en el ámbito estatal será aprobada por Resolución de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial y se publicará en el «Boletín Oficial del Estado» y en la sede electrónica del PAGe de la Administración General del Estado.

Sección 2.ª Identificación electrónica de las administraciones públicas y autenticación del ejercicio de su competencia

Artículo 18. *Identificación de las sedes electrónicas y de las sedes electrónicas asociadas.*

1. De acuerdo con lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas y sedes electrónicas asociadas utilizarán, para identificarse y garantizar

una comunicación segura con las mismas, certificados cualificados de autenticación de sitio web o medio equivalente. Dichos certificados electrónicos se ajustarán a lo señalado en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad, y la normativa vigente en materia de identidad y firma electrónica.

2. En el ámbito estatal las sedes electrónicas y sedes electrónicas asociadas se identificarán mediante certificados cualificados de autenticación de sitio web.

Con carácter adicional y para su identificación inmediata, los ciudadanos y ciudadanas dispondrán de la información general obligatoria que debe constar en las mismas de acuerdo con lo establecido en este Reglamento. Las direcciones electrónicas que tengan la condición de sede electrónica o sede electrónica asociada deberán hacerlo constar de forma visible e inequívoca. Para facilitar su identificación, seguirán las disposiciones generales que se establezcan para la imagen institucional de la Administración General del Estado y su dirección electrónica incluirá el nombre de dominio «.gob.es».

Artículo 19. *Identificación mediante sello electrónico basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.*

1. De acuerdo con lo previsto en el artículo 40 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán identificarse mediante el uso de un sello electrónico basado en un certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica. Estos certificados electrónicos incluirán el número de identificación fiscal y la denominación correspondiente, así como, en su caso, la identidad de la persona titular en el caso de los sellos electrónicos de órganos administrativos.

2. La relación de sellos electrónicos utilizados por cada Administración Pública, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos, publicándose en la sede electrónica o sede asociada o en el portal de internet correspondiente. Además, cada Administración Pública adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

3. En el ámbito estatal, la creación de sellos electrónicos se realizará mediante resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, que se publicará en la sede electrónica o sede electrónica asociada correspondiente. En dicha resolución deberá constar:

a) El órgano, organismo público o entidad de derecho público vinculado o dependiente titular del sello, que será el responsable de su utilización, con indicación de su Ministerio de adscripción, vinculación o dependencia.
b) Características técnicas generales del sistema de firma y certificado aplicable.
c) Servicio de validación para la verificación del certificado.
d) Actuaciones y procedimientos en los que podrá ser utilizado.

4. Los certificados de sello electrónico en el ámbito estatal tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».
b) Nombre del suscriptor.
c) Número de identificación fiscal del suscriptor.

Artículo 20. *Sistemas de firma electrónica para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42 de la Ley 40/2015, de 1 de octubre, en la tramitación administrativa automatizada de los procedimientos, cada Administración Pública podrá determinar los supuestos de utilización de los siguientes sistemas de firma electrónica:

a) Sello electrónico de Administración Pública, órgano, organismo público o entidad de derecho público, a que se refiere el artículo 19 de este Reglamento, basado en certificado electrónico cualificado que reúna los requisitos exigidos por la legislación de firma electrónica.
b) Código seguro de verificación vinculado a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos,

permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede electrónica correspondiente.

2. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes cuando estas tramiten procedimientos de forma automatizada en el ejercicio de potestades administrativas.

Artículo 21. *Sistemas de firma basados en código seguro de verificación para la actuación administrativa automatizada.*

1. De acuerdo con lo previsto en el artículo 42.b) de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas podrán utilizar sistemas de código seguro de verificación de documentos en el desarrollo de actuaciones automatizadas.

Dicho código vinculará al órgano, organismo público o entidad de derecho público y, en su caso, a la persona firmante del documento, permitiéndose en todo caso la comprobación de la integridad del documento en la sede electrónica o sede electrónica asociada correspondiente mediante un procedimiento de verificación directo y gratuito para las personas interesadas.

2. El sistema de código seguro de verificación deberá garantizar, en todo caso:

a) El origen e integridad de los documentos mediante el acceso a la sede electrónica o sede electrónica asociada correspondiente.

b) El carácter único del código generado para cada documento.

c) Su vinculación con el documento generado y, en su caso, con el firmante. El código seguro de verificación y la dirección electrónica de acceso a la sede electrónica o sede electrónica asociada deberán integrarse preferentemente en todas las páginas del documento firmado con dicho código. Cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente.

d) La posibilidad de verificar el documento en la sede electrónica o sede electrónica asociada, como mínimo, por el tiempo que se establezca en la resolución que autorice la utilización de este procedimiento. Una vez que el documento deje de estar disponible en la sede electrónica o sede electrónica asociada, su disponibilidad por otros cauces se regirá por lo dispuesto en la estrategia de conservación implantada por cada Administración Pública a través de su política de gestión documental.

e) Un acceso restringido al documento a quien disponga del código seguro de verificación, sin perjuicio de las garantías adicionales que se puedan establecer.

3. En las comunicaciones de documentos electrónicos a otros órganos, organismos o entidades y cuando así lo determinen las partes implicadas, la interoperabilidad se garantizará mediante la superposición al código seguro de verificación de un sello electrónico de los previstos en el artículo 42 de la Ley 40/2015, de 1 de octubre, como mecanismo de verificación automática del origen e integridad de los documentos electrónicos en los términos que establezca la Norma Técnica de Interoperabilidad de Documento Electrónico.

4. En el ámbito estatal, la utilización de este sistema requerirá resolución de la persona titular de la Subsecretaría del Ministerio o de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente, previo informe del Centro Criptológico Nacional y de la Secretaría General de Administración Digital.

La orden o resolución de creación deberá incluir:

a) Actuaciones a las que es de aplicación el sistema.

b) Órganos responsables de la aplicación del sistema.

c) Disposiciones que resultan de aplicación a la actuación.

d) Sede electrónica o sede electrónica asociada a la que pueden acceder las personas interesadas para la verificación del contenido de la actuación o documento.

e) Plazo de disponibilidad para la verificación en la sede electrónica o sede electrónica asociada del código seguro de verificación aplicado a un documento. Este plazo será al menos de cinco años, salvo que en la normativa especial por razón de la materia se prevea un plazo superior. Transcurrido este tiempo, será necesario solicitarlo al órgano de la

Administración Pública, organismo público o entidad de derecho público que emitió el documento. En este caso, cuando utilice medios electrónicos, la certificación de la verificación se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público que tenga atribuida la actuación por aquel órgano.

Artículo 22. *Sistemas de firma electrónica del personal al servicio de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 43 de la Ley 40/2015, de 1 de octubre, sin perjuicio de lo previsto en los artículos 18, 19 y 20 de este Reglamento, la actuación de una Administración Pública, organismo público o entidad de derecho público, cuando utilice medios electrónicos, se realizará mediante firma electrónica del titular del órgano competente o del empleado o empleada público a través del que se ejerza la competencia.

2. Cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal. Estos sistemas podrán identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios.

3. Los certificados electrónicos de empleado público serán cualificados y se ajustarán a lo señalado en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica.

4. Cada Administración determinará los medios admitidos para la firma electrónica en las entidades de derecho privado vinculadas o dependientes de esta cuando tramiten procedimientos en el ejercicio de potestades administrativas.

Artículo 23. *Certificados electrónicos de empleado público con número de identificación profesional.*

1. Sin perjuicio de lo previsto en el artículo 22.3 de este Reglamento, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, los prestadores cualificados de servicios de confianza podrán consignar un número de identificación profesional en el certificado electrónico de empleado público, a petición de la Administración en la que presta servicios el empleado o empleada de que se trate, si dicho certificado se va a utilizar en actuaciones que afecten a información clasificada, a la seguridad pública, a la defensa nacional o a otras actuaciones para cuya realización esté legalmente justificado el anonimato. Estos certificados se denominarán «certificados electrónicos de empleado público con número de identificación profesional».

2. En el ámbito estatal corresponderá solicitar la consignación de un número de identificación profesional del empleado o empleada público a la persona titular de la Subsecretaría del ministerio o a la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público en el que preste servicios el empleado o empleada público.

3. La Administración solicitante del certificado conservará la documentación acreditativa de la identidad del titular.

4. Los certificados electrónicos de empleado público con número de identificación profesional serán cualificados y se ajustarán a lo previsto en el Esquema Nacional de Interoperabilidad y la legislación vigente en materia de identidad y firma electrónica y tendrán idéntico uso, capacidad y funcionalidad que el certificado electrónico de empleado público, aunque limitados a las actuaciones que justificaron su emisión.

5. Las autoridades públicas competentes y los órganos judiciales, en el ejercicio de sus funciones y de acuerdo con la normativa vigente, podrán solicitar la revelación de la identidad del titular de un certificado de empleado público con número de identificación profesional mediante petición oficial dirigida a la Administración responsable de su custodia.

Artículo 24. *Sistemas de identificación y firma electrónica del personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. El personal al servicio de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, podrá identificarse con aquellos sistemas que, entre los previstos en la Ley 39/2015, de 1 de octubre, se

establezcan en función del nivel de seguridad que corresponda al trámite de que se trate de acuerdo al Esquema Nacional de Seguridad.

2. Dicho personal podrá firmar mediante sistemas de firma electrónica basados en certificados electrónicos cualificados facilitados específicamente a sus empleados y empleadas. Estos sistemas podrán ser utilizados por estos en el desempeño efectivo de su puesto de trabajo, para los trámites y actuaciones que realicen por razón del mismo, o para relacionarse con las Administraciones públicas cuando estas lo admitan.

3. Se podrá disponer de sistemas de identificación de personal basados en repositorios de empleados públicos que permitan la relación de los empleados y empleadas públicos con servicios y aplicaciones necesarios para el ejercicio de sus funciones que en todo caso garanticen lo previsto en el Esquema Nacional de Seguridad.

4. Los registros de personal de la Administración General del Estado podrán recoger los datos para la identificación electrónica de los empleados y empleadas públicos, así como su cesión a sistemas de identificación de personal basados en repositorios de identidades de empleados públicos.

Artículo 25. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. De acuerdo con lo previsto en el artículo 44 de la Ley 40/2015, de 1 de octubre, los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones Públicas, órganos, organismos públicos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en este artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a una misma Administración Pública, esta establecerá las condiciones y garantías por las que se regirá, que comprenderán, al menos, la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones Públicas, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio suscrito entre aquellas.

4. En el ámbito estatal, las condiciones y garantías a que se refiere el apartado 2 serán establecidas por la Secretaría General de Administración Digital.

5. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan conforme a los requisitos establecidos en el Esquema Nacional de Seguridad

Sección 3.ª Identificación y firma de las personas interesadas

Artículo 26. *Sistemas de identificación de las personas interesadas en el procedimiento.*

1. De acuerdo con lo previsto en la Ley 39/2015, de 1 de octubre, los interesados podrán identificarse electrónicamente ante las Administraciones Públicas a través de cualquier sistema que cuente con un registro previo como usuario que permita garantizar su identidad.

2. En particular, de acuerdo con lo previsto en el artículo 9.2 de la Ley 39/2015, de 1 de octubre, serán admitidos los siguientes sistemas de identificación electrónica:

a) Sistemas basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas basados en certificados electrónicos cualificados de sello electrónico expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Sistemas de clave concertada y cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad, previa autorización por parte de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todo procedimiento, aun cuando se admita para ese mismo procedimiento alguno de los previstos en la letra c).

Artículo 27. *Atributos mínimos de los certificados electrónicos cuando se utilizan para la identificación de las personas interesadas ante las Administraciones Públicas.*

1. Los sistemas basados en certificados cualificados de firma electrónica admitidos por las Administraciones Públicas para la identificación electrónica de persona física a que se refiere el artículo 9.2.a) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener como atributos, al menos, su nombre y apellidos y su número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal que conste como tal de manera inequívoca. La comprobación de la identidad y otras circunstancias de los solicitantes del certificado, se realizará de conformidad con lo previsto en el artículo 7 de la Ley 6/2020, de 11 de noviembre.

2. Los certificados electrónicos cualificados de representante de persona jurídica deberán contener, como mínimo, la denominación y el Número de Identificación Fiscal de la persona jurídica y el nombre y apellidos y número de Documento Nacional de Identidad, o Número de Identificación de Extranjero o Número de Identificación Fiscal de la persona que actúa como representante.

3. Los sistemas basados en certificados cualificados de sello electrónico admitidos por las Administraciones Públicas para la identificación electrónica de persona jurídica a que se refiere el artículo 9.2.b) de la Ley 39/2015, de 1 de octubre, emitidos al amparo de la Ley 6/2020, de 11 de noviembre, deberán contener, como mínimo, su denominación y su Número de Identificación Fiscal.

Artículo 28. *Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas.*

1. Los sistemas de clave concertada o cualquier otro sistema que las Administraciones Públicas consideren válidos, admitidos para la identificación electrónica de persona física de conformidad con el artículo 9.2.c) de la Ley 39/2015, de 1 de octubre, deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad y contener, como mínimo, el nombre y apellidos y el número de Documento Nacional de Identidad, Número de Identificación de Extranjero, Número de Identificación Fiscal y, para los casos en que así se establezca en la definición del sistema, el número de pasaporte.

2. Los sistemas de identificación a que se refiere el apartado anterior deberán ser autorizados previamente por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior.

3. En el ámbito estatal, la creación de los nuevos sistemas de identificación será aprobada por orden de la persona titular del Ministerio o, en su caso, resolución de la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público vinculado o dependiente por razón del ámbito material en que se vaya a utilizar, previa autorización de la Secretaría General de Administración Digital a que se refiere el apartado anterior.

Cuando el nuevo sistema se refiera a la totalidad de la Administración General del Estado se requerirá Acuerdo del Consejo de Ministros a propuesta de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En este caso, este sistema deberá estar accesible a través de la Plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

Artículo 29. *Sistemas de firma electrónica de las personas interesadas admitidos por las Administraciones Públicas y régimen de uso.*

1. De acuerdo con lo previsto en el artículo 10.2 de la Ley 39/2015, de 1 de octubre, en el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico incluidos en la «Lista de confianza de prestadores cualificados de servicios de confianza».

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezca, siempre que cuente con un registro previo como usuario que permita garantizar su identidad.

Las Administraciones Públicas deberán garantizar que la utilización de uno de los sistemas previstos en las letras a) y b) sea posible para todos los procedimientos en todos sus trámites, aun cuando adicionalmente se permita alguno de los previstos al amparo de lo dispuesto en la letra c).

2. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación del interesado y, en su caso, del representante o la representante, que sean necesarios de acuerdo con la legislación que le sea aplicable.

3. Los sistemas de firma electrónica que usen las personas interesadas permitirán que las Administraciones Públicas puedan verificar los datos consignados de la firma, de manera que se pueda vincular su identidad con el acto de firma.

4. Los sistemas de firma electrónica previstos en la letra c) del apartado 1 deberán contar con la previa autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, que solo podrá ser denegada por motivos de seguridad pública, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior. Asimismo, deberán cumplir con lo previsto en el Real Decreto 3/2010, de 8 de enero.

5. De acuerdo con lo previsto en el artículo 10.4 de la Ley 39/2015, de 1 de octubre, cuando así lo disponga expresamente la normativa reguladora aplicable, las Administraciones Públicas podrán admitir los sistemas de identificación previstos en dicha ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de las personas interesadas.

Artículo 30. *Identificación o firma electrónica de las personas interesadas mediante personal funcionario público habilitado.*

1. De acuerdo con lo previsto en el segundo párrafo del artículo 12.2 de la Ley 39/2015 de 1 de octubre, si algún interesado no incluido en los apartados 2 y 3 del artículo 14 de la ley no dispusiera de los medios electrónicos necesarios para su identificación o firma electrónica en el procedimiento administrativo, estas podrán ser válidamente realizadas por personal funcionario público habilitado mediante el uso del sistema de firma electrónica del que esté dotado para ello. En este caso, será necesario que el interesado se identifique ante el funcionario o funcionaria y preste su consentimiento expreso para esta actuación, de lo que deberá quedar constancia por escrito para los casos de discrepancia o litigio.

El funcionario habilitado entregará al interesado toda la documentación acreditativa del trámite realizado, así como una copia del documento de consentimiento expreso cumplimentado y firmado, cuyo formulario estará disponible en el Punto de Acceso General Electrónico de la respectiva Administración

2. En el ámbito estatal la identificación y firma electrónica del interesado conforme al procedimiento descrito en el apartado anterior se realizará necesariamente por un funcionario público inscrito a tal efecto en el Registro de Funcionarios Habilitados de la Administración General del Estado.

La identificación o firma electrónica en el procedimiento por personal funcionario público habilitado sólo será válida para los trámites y actuaciones que haya determinado con carácter previo cada ministerio, organismo público o entidad de derecho público vinculado o dependiente y en los términos que se especifiquen mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital. En el PAGe de la Administración General del Estado y en las sedes electrónicas asociadas de cada ministerio o en la sede electrónica o sede asociada del organismo público o entidad de derecho público en su ámbito de competencia, se mantendrá una relación pública, permanentemente actualizada, de dichos trámites y actuaciones.

Artículo 31. *Registro de Funcionarios Habilitados de la Administración General del Estado.*

1. Se crea el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, en el que constarán inscritos:

a) El personal funcionario habilitado para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen por el ministerio, organismo o entidad competente para su tramitación.

b) El personal funcionario habilitado para la expedición de copias auténticas. Esta habilitación será conferida por los órganos a los que corresponda la emisión de los documentos originales, su custodia, el archivo de documentos o que en sus normas de competencia así se haya previsto.

c) El personal funcionario habilitado que presta servicio en las oficinas de asistencia en materia de registros de la Administración General del Estado, que estará habilitados para la identificación y firma electrónica de las personas interesadas en aquellos trámites y procedimientos que se determinen y para la expedición de copias auténticas electrónicas de cualquier documento que estas presenten para que se remita desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. El Registro de Funcionarios Habilitados será gestionado por la Secretaría de Estado de Política Territorial y Función Pública del Ministerio de Política Territorial y Función Pública, en colaboración con la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital. Este Registro será interoperable con los sistemas equivalentes que ya existan en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

3. Este Registro deberá ser plenamente interoperable con los registros u otros sistemas equivalentes que se creen por las comunidades autónomas y las entidades locales a los efectos de comprobar la validez de las citadas habilitaciones.

4. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regulará el funcionamiento del Registro de Funcionarios Habilitados

Sección 4.ª Acreditación de la representación de las personas interesadas

Artículo 32. *Acreditación en la actuación por medio de representante.*

1. De acuerdo con lo previsto en el artículo 5 de la Ley 39/2015, de 1 de octubre, las personas interesadas con capacidad de obrar podrán actuar ante las Administraciones Públicas por medio de representante, bien sea una persona física con capacidad de obrar bien sea una persona jurídica cuando así esté previsto en sus Estatutos.

2. Los representantes de las personas interesadas obligadas a relacionarse electrónicamente con las Administraciones Públicas están obligados a relacionarse electrónicamente en el ejercicio de dicha representación, de acuerdo con el artículo 14.2 de la Ley 39/2015, de 1 de octubre.

3. La representación puede acreditarse mediante cualquier medio válido en Derecho que deje constancia fidedigna de su existencia, entre otros:

a) Mediante apoderamiento apud acta efectuado por comparecencia personal en las oficinas de asistencia en materia de registros o comparecencia electrónica en la correspondiente sede electrónica o sede electrónica asociada.

b) Mediante acreditación de su inscripción en el registro electrónico de apoderamientos de la Administración Pública competente o en sus registros particulares de apoderamientos.

c) Mediante un certificado electrónico cualificado de representante.

d) Mediante documento público cuya matriz conste en un archivo notarial o de una inscripción practicada en un registro mercantil.

4. En el caso de actuaciones en nombre de persona jurídica, la capacidad de representación podrá acreditarse también mediante certificado electrónico cualificado de representante, entendiéndose en tal caso que el poder de representación abarca cualquier actuación ante cualquier Administración Pública.

5. Asimismo, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, las Administraciones Públicas podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones por medios electrónicos en representación de las personas interesadas. En la sede electrónica o sede electrónica asociada de cada una de las Administraciones Públicas se publicarán los trámites electrónicos que podrán realizarse con esta representación.

Artículo 33. *Registro Electrónico de Apoderamientos de la Administración General del Estado.*

1. A los efectos previstos en el artículo anterior y de acuerdo con el artículo 6 de la Ley 39/2015, de 1 de octubre, en el Registro Electrónico de Apoderamientos de la Administración General del Estado se inscribirán los apoderamientos de carácter general previstos en el artículo 6.4.a) de dicha ley otorgados «apud acta» a favor de representante, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo para actuar en su nombre ante las Administraciones Públicas.

Asimismo, podrán inscribirse los poderes previstos en el artículo 6.4.b) de la ley para actuar ante la Administración General del Estado o ante un organismo público o entidad de Derecho Público vinculado o dependiente de la misma que no cuente con un registro electrónico de apoderamientos particular. Por último, podrán inscribirse los poderes previstos en el artículo 6.4.c) de la ley otorgados para realizar determinados trámites y actuaciones especificados en el poder ante los órganos de la Administración General del Estado o ante un organismo público o entidad de derecho público vinculado o dependiente de dicha Administración que no cuente con el citado registro particular.

Constará en el Registro el bastanteo del poder realizado por los servicios jurídicos correspondientes, sin perjuicio de la apreciación concreta de su suficiencia en la actuación, trámite o procedimiento en que se emplee.

2. El Registro Electrónico de Apoderamientos de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública con la colaboración del Ministerio de Asuntos Económicos y Transformación Digital, y será accesible desde la sede electrónica del PAGe de la Administración General del Estado así como desde las sedes y sedes electrónicas asociadas de la Administración General del Estado y de los organismos públicos o entidades de derecho público vinculados o dependientes.

3. Sin perjuicio de este registro general de apoderamientos, cada organismo público o entidad de derecho público vinculado o dependiente de la Administración General del Estado podrá disponer de un registro particular de apoderamientos en el que se inscriban los poderes otorgados por quien ostente la condición de interesado para realizar los trámites específicos de su competencia y cuya gestión corresponderá al propio organismo o entidad.

En estos registros particulares no podrán inscribirse los poderes previstos en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

4. El Registro Electrónico de Apoderamientos y los registros particulares deberán ser interoperables y no tienen carácter público, por lo que el interesado sólo podrá acceder a la información de los apoderamientos de los que sea poderdante o apoderado.

5. Mediante orden conjunta de la persona titular del Ministerio de Política Territorial y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y

Transformación Digital se regularán los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos de la Administración General del Estado.

Artículo 34. *Acreditación de la representación mediante certificado electrónico cualificado de representante.*

1. La representación podrá acreditarse ante la Administración con un certificado electrónico cualificado de representante de persona jurídica que sea acorde a lo previsto en el artículo 28 y el Anexo I del al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (en adelante, Reglamento eIDAS) y a la Política marco de Firma Electrónica y de certificados a que hace referencia el Esquema Nacional de Interoperabilidad y, además, haya sido expedido a quien tenga un poder general para llevar a cabo cualquier actuación administrativa y ante cualquier Administración.

2. La aceptación de certificados electrónicos cualificados de representante de persona jurídica de alcance no general estará sujeta al Reglamento eIDAS, a la Política Marco de Firma Electrónica y de Certificados a que hace referencia el Esquema Nacional de Interoperabilidad y además, a los requisitos que disponga cada Administración.

Artículo 35. *Acreditación y verificación de las representaciones que resulten de un documento público notarial o certificación de un Registro Mercantil.*

1. Cuando la representación alegada resulte de un documento público notarial, o de una certificación expedida por un registro mercantil, el interesado deberá aportar la certificación registral electrónica correspondiente o al menos expresar el código seguro u otro sistema de acceso y verificación del documento electrónico.

2. Las Administraciones Públicas efectuarán la verificación de la autenticidad e integridad del traslado a papel y el acceso a los metadatos necesarios para la tramitación automatizada de la certificación registral electrónica, mediante el acceso electrónico y gratuito a la dirección electrónica que el Consejo General del Notariado o el Colegio de Registradores, respectivamente, habrán de tener habilitada a tales efectos.

3. Asimismo, las Administraciones Públicas, cuando necesiten comprobar la vigencia, revocación o cese de representaciones inscritas en el Registro Mercantil, consultarán electrónicamente y de modo gratuito el Registro Mercantil.

Artículo 36. *Autorización de representantes de terceros por la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.*

1. La Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, de acuerdo con lo previsto en el artículo 5.7 de la Ley 39/2015, de 1 de octubre, podrán habilitar con carácter general o específico a personas físicas o jurídicas autorizadas para la realización de determinadas transacciones electrónicas en representación de las personas interesadas.

2. La habilitación requerirá la firma previa de un convenio entre el Ministerio, organismo público o entidad de derecho público vinculado o dependiente competente y la organización o corporación de que se trate, de acuerdo de lo previsto en el capítulo VI del título Preliminar de la Ley 40/2015, de 1 de octubre. El convenio deberá especificar, al menos, los procedimientos y trámites objeto de la habilitación, y las condiciones y obligaciones aplicables tanto a la entidad firmante del convenio, como a las personas físicas o jurídicas habilitadas y determinará la presunción de validez de la representación.

A estos efectos, podrá acordarse un modelo normalizado de convenio que permita dar soporte a esta habilitación en los términos y condiciones que las partes acuerden, conforme a lo dispuesto en la Ley 40/2015, de 1 de octubre, y que incluya como anexo el modelo individualizado de adhesión al convenio que, previendo expresamente la aceptación de su contenido íntegro, deben suscribir las personas físicas o jurídicas miembros de las organizaciones o corporaciones firmantes que se adhieran al mismo.

3. De acuerdo con lo previsto en el artículo 32.5, en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, los trámites electrónicos que podrán realizarse con esta representación se publicarán en la sede electrónica del PAGe de la Administración General del Estado y en las respectivas sedes electrónicas o sedes electrónicas asociadas.

CAPÍTULO III

Registros, comunicaciones y notificaciones electrónicas

Sección 1.ª Registros electrónicos

Artículo 37. *Registro electrónico.*

1. Las Administraciones Públicas dispondrán de registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones, que deberán ser plenamente interoperables de manera que se garantice su compatibilidad informática e interconexión en los términos previstos en el artículo 16 de la Ley 39/2015, de 1 de octubre y en el artículo 60 de este Reglamento.

2. Cada Administración dispondrá de un Registro Electrónico General en el que hará el asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad de derecho público vinculado o dependiente. Los organismos públicos y entidades de derecho público vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración a la que estén vinculados o de la que dependan.

3. Los registros electrónicos admitirán:

a) Documentos electrónicos normalizados correspondientes a los servicios, procedimientos y trámites que se especifiquen conforme a lo dispuesto en la norma de creación del registro, cumplimentados de acuerdo con formatos preestablecidos.

b) Cualquier solicitud, escrito o comunicación distinta de los mencionados en el párrafo anterior dirigido a cualquier Administración Pública.

4. De acuerdo con el artículo 16.8 de la Ley 39/2015, de 1 de octubre, no se tendrán por presentados en el registro aquellos documentos e información cuyo régimen especial establezca otra forma de presentación. En estos supuestos, el órgano administrativo competente para la tramitación del procedimiento comunicará esta circunstancia al interesado e informará de los requisitos exigidos por la legislación específica aplicable

Artículo 38. *Registro Electrónico General de la Administración General del Estado.*

1. El Registro Electrónico General de la Administración General del Estado será gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital y se configura como el conjunto agregado de:

a) Los asientos practicados a través de las aplicaciones de que dispongan las unidades que realicen anotaciones en registro.

b) Las anotaciones que se realicen en cualquier aplicación que proporcione soporte a procedimientos específicos.

c) Las anotaciones que se practiquen por medio del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones que no dispongan de modelos normalizados de presentación, independientemente de las Administraciones Públicas u organismos públicos o entidades de derecho público vinculados o dependientes a las que vayan dirigidos. Dicho servicio electrónico será accesible desde la sede electrónica del PAGe de la Administración General del Estado.

2. Las anotaciones en el Registro General de la Administración General del Estado tendrán plena eficacia y validez para todas las Administraciones Públicas.

Artículo 39. *Presentación y tratamiento de documentos en registro.*

1. Las Administraciones Públicas podrán determinar los formatos y estándares a los que deberán ajustarse los documentos presentados por las personas interesadas en el registro siempre que cumplan con lo previsto en el Esquema Nacional de Interoperabilidad y normativa correspondiente.

2. En el caso de que se detecte código malicioso susceptible de afectar a la integridad o seguridad del sistema en documentos que ya hayan sido registrados, se requerirá su subsanación al interesado que los haya aportado de acuerdo con lo previsto en el artículo 14.3 de este Reglamento.

3. Los documentos en soporte no electrónico se presentarán a través de las oficinas de asistencia en materia de registros. Cuando se presenten documentos originales o copias auténticas en soporte no electrónico, desde el momento en que sean digitalizados conforme a lo dispuesto en las correspondientes normas técnicas de interoperabilidad, tendrán la consideración de copia electrónica auténtica de documento en soporte papel con la misma validez para su tramitación que los documentos aportados en soporte papel, conforme a las previsiones del artículo 27 de la Ley 39/2015, de 1 de octubre.

4. Cuando el tamaño de los documentos registrados exceda la capacidad que se determine para el Sistema de Interconexión de Registros (SIR), su remisión a la Administración y órgano al que van dirigidos podrá sustituirse por la puesta a disposición de los documentos, previamente depositados en un repositorio de intercambio de ficheros.

En ámbito de la Administración General del Estado dicho repositorio de intercambio de ficheros será de titularidad pública y tanto los documentos depositados como los datos que estos contengan no podrán ser utilizados para fines distintos a los previstos en la normativa que regule el procedimiento para el que han sido objeto de registro.

5. Los documentos presentados en las oficinas de asistencia en materia de registro serán devueltos a las personas interesadas inmediatamente tras su digitalización o, en caso contrario, se les aplicará lo previsto en el artículo 53 de este Reglamento.

6. El archivo de los documentos intercambiados por registro corresponderá al órgano competente para la tramitación del procedimiento, de acuerdo al plazo que determine su normativa.

Artículo 40. *Oficinas de asistencia en materia de registros en el ámbito de la Administración General del Estado.*

1. Las Oficinas de asistencia en materia de registros tienen naturaleza de órgano administrativo de acuerdo con lo dispuesto en el artículo 5 de la Ley 40/2015, de 1 de octubre.

La creación de nuevas Oficinas, así como la modificación o supresión de las existentes se realizará conforme a lo previsto en el artículo 59.2 de la Ley 40/2015, de 1 de octubre.

2. La Administración General del Estado contará con un directorio geográfico de las Oficinas de asistencia en materia de registros que será gestionado por el Ministerio de Política Territorial y Función Pública. A tal efecto, el órgano del que dependa la correspondiente Oficina de asistencia deberá comunicar de forma inmediata al citado Ministerio la aprobación de la norma por la que se cree, modifique o suprima dicha oficina, de acuerdo con lo establecido en el Esquema Nacional de Interoperabilidad, garantizando su actualización permanente.

3. Las Oficinas de asistencia en materia de registros desarrollarán las siguientes funciones:

a) La digitalización de las solicitudes, escritos y comunicaciones en papel que se presenten o sean recibidos en la Oficina y se dirijan a cualquier órgano, organismo público o entidad de derecho público de cualquier Administración Pública, así como su anotación en el Registro Electrónico General o Registro electrónico de cada organismo o entidad según corresponda.

b) La anotación, en su caso, de los asientos de salida que se realicen de acuerdo con lo dispuesto en el artículo 16 de la Ley 39/2015, de 1 de octubre.

c) La emisión del correspondiente recibo que acredite la fecha y hora de presentación de solicitudes, comunicaciones y documentos que presenten las personas interesadas.

d) La expedición de copias electrónicas auténticas tras la digitalización de cualquier documento original o copia auténtica que presenten las personas interesadas y que se vaya a incorporar a un expediente administrativo a través de dicha oficina en el registro electrónico correspondiente.

e) La información en materia de identificación y firma electrónica, para la presentación de solicitudes, escritos y comunicaciones a través de medios electrónicos en los trámites y procedimientos para los que se haya conferido habilitación.

f) La identificación o firma electrónica del interesado, cuando se trate de una persona no obligada a la relación electrónica con la Administración, en los procedimientos administrativos para los que se haya previsto habilitación.

g) La práctica de notificaciones, en el ámbito de actuación de esa Oficina, cuando el interesado o su representante comparezcan de forma espontánea en la Oficina y solicite la comunicación o notificación personal en ese momento.

h) La comunicación a las personas interesadas del código de identificación del órgano, organismo público o entidad a la que se dirige la solicitud, escrito o comunicación.

i) La iniciación de la tramitación del apoderamiento presencial apud acta en los términos previstos en el artículo 6 de la Ley 39/2015, de 1 de octubre.

j) Cualesquiera otras funciones que se les atribuyan legal o reglamentariamente.

Sección 2.ª Comunicaciones y notificaciones electrónicas

Artículo 41. *Comunicaciones administrativas a las personas interesadas por medios electrónicos.*

Cuando de acuerdo con lo previsto en el artículo 14 de la Ley 39/2015, de 1 de octubre, la relación de las personas interesadas con las Administraciones Públicas deba realizarse por medios electrónicos, serán objeto de comunicación al interesado por medios electrónicos, al menos:

a) La fecha y, en su caso, hora efectiva de inicio del cómputo de plazos que haya de cumplir la Administración tras la presentación del documento o documentos en el registro electrónico, de acuerdo con lo previsto en el artículo 31.2.c) de la Ley 39/2015, de 1 de octubre.

b) La fecha en que la solicitud ha sido recibida en el órgano competente, el plazo máximo para resolver el procedimiento y para la práctica de la notificación de los actos que le pongan término, así como de los efectos del silencio administrativo, de acuerdo con lo previsto en el artículo 21.4 de la Ley 39/2015, de 1 de octubre.

c) La solicitud de pronunciamiento previo y preceptivo a un órgano de la Unión Europea y la notificación del pronunciamiento de ese órgano de la Unión Europea a la Administración instructora de acuerdo con lo previsto en el artículo 22.1.b) de la Ley 39/2015, de 1 de octubre.

d) La existencia, desde que se tenga constancia de la misma, de un procedimiento no finalizado en el ámbito de la Unión Europea que condicione directamente el contenido de la resolución, así como la finalización de dicho procedimiento de acuerdo con lo previsto en el artículo 22.1.c) de la Ley 39/2015, de 1 de octubre.

e) La solicitud de un informe preceptivo a un órgano de la misma o distinta Administración y la recepción, en su caso, de dicho informe, de acuerdo con lo previsto en el artículo 22.1.d) de la Ley 39/2015, de 1 de octubre.

f) La solicitud de previo pronunciamiento de un órgano jurisdiccional, cuando este sea indispensable para la resolución del procedimiento, así como el contenido del pronunciamiento cuando la Administración actuante tenga la constancia del mismo de acuerdo con lo previsto en el artículo 22.1.g) de la Ley 39/2015, de 1 de octubre.

g) La realización del requerimiento de anulación o revisión de actos entre administraciones previsto en el artículo 22.2.a) de la Ley 39/2015, de 1 de octubre, así como su cumplimiento o, en su caso, la resolución del correspondiente recurso contencioso-administrativo.

Artículo 42. *Práctica de las notificaciones a través de medios electrónicos.*

1. De acuerdo con lo previsto en el artículo 43.1 de la Ley 39/2015, de 1 de octubre, las notificaciones por medios electrónicos se practicarán mediante comparecencia en la sede electrónica o sede electrónica asociada de la Administración, organismo público o entidad de derecho público vinculado o dependiente actuante, a través de la Dirección Electrónica Habilitada única o mediante ambos sistemas, según disponga cada Administración, organismo público o entidad de derecho público vinculado o dependiente, debiendo quedar constancia de la fecha y hora del acceso al contenido de la misma, o del rechazo de la notificación.

En caso de que la Administración, organismo o entidad actuante lleve a cabo la puesta a disposición de las notificaciones por ambos sistemas, para el cómputo de plazos y el resto de efectos jurídicos se tomará la fecha y hora de acceso al contenido o el rechazo de la notificación por el interesado o su representante en el sistema en el que haya ocurrido en primer lugar. A tal efecto se habrá de disponer de los medios electrónicos necesarios para sincronizar de forma automatizada en uno y otro sistema la información sobre el estado de la notificación con objeto de garantizar la eficacia y seguridad jurídica en la tramitación del procedimiento.

2. Con independencia de que un interesado no esté obligado a relacionarse electrónicamente con las Administraciones Públicas o de que no haya comunicado que se le practiquen notificaciones por medios electrónicos, su comparecencia voluntaria o la de su representante en la sede electrónica o sede asociada de una Administración, organismo público o entidad de derecho público vinculado o dependiente o a través de la Dirección Electrónica Habilitada única, y el posterior acceso al contenido de la notificación o el rechazo expreso de esta tendrá plenos efectos jurídicos.

3. La notificación por comparecencia en la sede electrónica o sede electrónica asociada y a través de la Dirección Electrónica Habilitada única conlleva la puesta a disposición del interesado de un acuse de recibo que permita justificar bien el acceso al contenido de la notificación, bien el rechazo del interesado a recibirla.

El acuse contendrá, como mínimo, la identificación del acto notificado y la persona destinataria, la fecha y hora en la que se produjo la puesta a disposición y la fecha y hora del acceso a su contenido o del rechazo.

4. En los supuestos de sucesión de personas físicas o jurídicas, inter vivos o mortis causa, la persona o entidad que sucede al interesado comunicará la sucesión al órgano competente de la tramitación del procedimiento de cuya existencia tenga conocimiento. Dicha comunicación deberá efectuarse tras la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física.

El órgano responsable de la tramitación procederá, en su caso, en procedimientos no finalizados, a autorizar a la persona o entidad sucesora el acceso a las notificaciones electrónicas ya practicadas desde la fecha del hecho causante de la sucesión y a practicar a dicha persona o entidad sucesora las notificaciones electrónicas que se produzcan en lo sucesivo. En el caso en el que la persona física sucesora no estuviera obligada a relacionarse electrónicamente con la Administración y no opte por este cauce de relación, las notificaciones que se produzcan en lo sucesivo deberán practicarse en papel, sin perjuicio de la garantía de acceso al expediente completo.

La persona o entidad que suceda al interesado en un procedimiento del que conozca su existencia debe comunicar, conforme a lo expuesto en los párrafos anteriores, la sucesión a la Administración Pública a la que corresponda la tramitación de aquel, en el plazo de 15 días hábiles, desde el día siguiente al de la efectividad de la sucesión o desde la inscripción de la defunción en el Registro Civil, en el caso de fallecimiento de persona física. Si la persona o entidad sucesora efectúa la comunicación después de dicho plazo, los defectos en la práctica de notificaciones que se deriven de este incumplimiento, que hubieran acaecido con anterioridad a dicha comunicación, le serán imputables al interesado; dándose por cumplida por la Administración, a todos los efectos, la obligación de puesta a disposición de la notificación electrónica en la sede electrónica o sede electrónica asociada, a través de la Dirección Electrónica Habilitada única o ambas, según proceda, a la persona jurídica o persona física cuya sucesión el interesado no ha hecho valer.

5. Toda notificación cuyo emisor pertenezca al ámbito estatal a que se refiere el artículo 1.2 de este Reglamento se pondrá a disposición del interesado a través de la Dirección Electrónica Habilitada única, incluyendo el supuesto previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre. Asimismo, los emisores de ámbito estatal podrán notificar en su sede electrónica o sede electrónica asociada de forma complementaria a la puesta a disposición en la Dirección Electrónica Habilitada única.

Artículo 43. *Aviso de puesta a disposición de la notificación.*

1. De acuerdo con lo previsto en el artículo 41.6 de la Ley 39/2015, de 1 de octubre, con independencia de que la notificación se realice en papel o por medios electrónicos, las Administraciones Públicas, organismos públicos o entidades de derecho público vinculados o dependientes enviarán al interesado o, en su caso, a su representante, aviso informándole de la puesta a disposición de la notificación bien en la Dirección Electrónica Habilitada única, bien en la sede electrónica o sede electrónica asociada de la Administración, u Organismo o Entidad o, en su caso, en ambas.

La falta de práctica de este aviso, de carácter meramente informativo, no impedirá que la notificación sea considerada plenamente válida.

El aviso se remitirá al dispositivo electrónico o la dirección de correo electrónico que el interesado haya comunicado voluntariamente al efecto, o a ambos, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre.

El interesado se hace responsable, por la comunicación a la Administración, organismo público o entidad de derecho público vinculado o dependiente, de que dispone de acceso al dispositivo o dirección de correo electrónico designados. En caso de que dejen de estar operativos o pierda la posibilidad de acceso, el interesado está obligado a comunicar a la Administración que no se realice el aviso en tales medios. El incumplimiento de esta obligación por parte del interesado no conllevará responsabilidad alguna para la Administración por los avisos efectuados a dichos medios no operativos.

El aviso regulado en este apartado sólo se practicará en caso de que el interesado o su representante hayan comunicado a la Administración un dispositivo electrónico o dirección de correo electrónico al efecto.

2. Cuando el interesado sea un sujeto obligado a relacionarse por medios electrónicos y la Administración emisora de la notificación no disponga de datos de contacto electrónicos para practicar el aviso de su puesta a disposición, en los procedimientos iniciados de oficio la primera notificación que efectúe la Administración, organismo o entidad se realizará en papel en la forma determinada por el artículo 42.2 de la Ley 39/2015, de 1 de octubre, advirtiendo al interesado en esa primera notificación que las sucesivas se practicarán en forma electrónica por comparecencia en la sede electrónica o sede electrónica asociada que corresponda o, en su caso, a través de la Dirección Electrónica Habilitada única según haya dispuesto para sus notificaciones la Administración, organismo o entidad respectivo, y dándole a conocer que, de acuerdo con lo previsto en el artículo 41.1 de la Ley 39/2015, de 1 de octubre, puede identificar un dispositivo electrónico, una dirección de correo electrónico o ambos para el aviso de la puesta a disposición de las notificaciones electrónicas posteriores.

3. Las Administraciones podrán crear bases de datos de contacto electrónico para la práctica de los avisos de puesta a disposición de notificaciones en su respectivo ámbito.

Artículo 44. *Notificación a través de la Dirección Electrónica Habilitada única.*

1. La Dirección Electrónica Habilitada única es el sistema de información para la notificación electrónica cuya gestión corresponde al Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública.

2. De acuerdo con lo previsto en el artículo 7.4, la Dirección Electrónica Habilitada única se aloja en la sede electrónica del PAGe de la Administración General del Estado.

3. La adhesión a la Dirección Electrónica Habilitada única se realizará en los términos previstos en el artículo 65.

Todas las Administraciones Públicas y sus organismos públicos y entidades de derecho público vinculados o dependientes colaborarán para establecer sistemas interoperables que

permitan que las personas físicas y jurídicas puedan acceder a todas sus notificaciones a través de la Dirección Electrónica Habilitada única, tal como establece el artículo 43 de la Ley 39/2015, de 1 de octubre.

Esta previsión será aplicable con independencia de cuál sea la Administración que practica la notificación y si las notificaciones se han practicado en papel o por medios electrónicos.

4. Cuando una incidencia técnica imposibilite el funcionamiento ordinario de la Dirección Electrónica Habilitada única, una vez comunicada dicha incidencia a los órganos, organismos o entidades emisores que la utilicen como medio de notificación, estos podrán determinar una ampliación del plazo no vencido para comparecer y acceder a las notificaciones emitidas. En caso de que también pongan a disposición las notificaciones en su sede electrónica o sede electrónica asociada, deberán publicar también en esta tanto la incidencia técnica acontecida en la Dirección Electrónica Habilitada única como la ampliación concreta, en su caso, del plazo no vencido.

5. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la Dirección Electrónica Habilitada única, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, dicho acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma, dará por efectuado el trámite de notificación y se continuará el procedimiento.

6. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la Dirección Electrónica Habilitada única deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la Dirección Electrónica Habilitada única se sincronizará automáticamente con la sede electrónica o sede electrónica asociada en la que, en su caso, la notificación también se hubiera puesto a disposición del interesado.

Artículo 45. *Notificación electrónica en sede electrónica o sede electrónica asociada.*

1. Con carácter previo al acceso al contenido de la notificación puesta a disposición del interesado en la sede electrónica o sede electrónica asociada del emisor de la misma, este será informado de que de acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1 de octubre, la comparecencia y acceso al contenido, el rechazo expreso de la notificación o bien la presunción de rechazo por haber transcurrido el plazo de diez días naturales desde la puesta a disposición de la notificación sin acceder al contenido de la misma dará por efectuado el trámite de notificación y se continuará el procedimiento.

2. Para dar por efectuado el trámite de notificación a efectos jurídicos, en la sede electrónica o sede electrónica asociada deberá quedar constancia, con indicación de fecha y hora, del momento del acceso al contenido de la notificación, del rechazo expreso de la misma o del vencimiento del plazo previsto en el artículo 43.2 de la Ley 39/2015, de 1 de octubre.

El estado del trámite de notificación en la sede electrónica o sede electrónica asociada se sincronizará automáticamente con la Dirección Electrónica Habilitada única si la notificación también se hubiera puesto a disposición del interesado en aquella.

3. De conformidad con el artículo 43.3 de la Ley 39/2015, de 1 de octubre, se entenderá cumplida la obligación de notificar en plazo por parte de la Administración, a que se refiere el artículo 40.4 de dicha ley, con la puesta a disposición de la notificación en la sede o en la dirección electrónica habilitada única.

TÍTULO III

Expediente administrativo electrónico

CAPÍTULO I

Documento administrativo electrónico y copias

Artículo 46. *Documento administrativo electrónico.*

1. Se entiende por documento administrativo electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico, según un formato determinado y susceptible de identificación y tratamiento diferenciado admitido en el Esquema Nacional de Interoperabilidad y normativa correspondiente, y que haya sido generada, recibida o incorporada por las Administraciones Públicas en el ejercicio de sus funciones sujetas a Derecho administrativo.

2. Cuando en el marco de un procedimiento administrativo tramitado por medios electrónicos el órgano actuante esté obligado a facilitar al interesado un ejemplar de un documento administrativo electrónico, dicho documento se podrá sustituir por la entrega de los datos necesarios para su acceso por medios electrónicos adecuados.

Artículo 47. *Requisitos de validez y eficacia de las copias auténticas de documentos.*

1. De acuerdo con lo previsto en el artículo 27.2 de la Ley 39/2015, de 1 de octubre, tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido.

2. Las copias auténticas se expedirán siempre a partir de un original o de otra copia auténtica y tendrán la misma validez y eficacia que los documentos originales.

Artículo 48. *Órganos competentes para la emisión de copias auténticas de documentos en el ámbito estatal.*

1. En el ámbito estatal, serán competentes para la expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original los siguientes órganos:

a) Los órganos a los que corresponda la emisión de los documentos originales.
b) Los órganos a los que corresponda la custodia y archivo de documentos.
c) Los órganos que hayan previsto sus normas de competencia.
d) Las oficinas de asistencia en materia de registros, respecto de los documentos originales o copias auténticas presentados por las personas interesadas para que se remitan desde la Oficina a la unidad competente para su incorporación a un expediente administrativo.

2. La expedición de copias auténticas de documentos públicos administrativos o documentos privados, que sean documentos originales o copias auténticas de documento original, podrá llevarse a cabo mediante actuación administrativa automatizada o por personal funcionario habilitado inscrito en el Registro de Funcionarios Habilitados de la Administración General del Estado al que se refiere el artículo 31 de este Reglamento.

3. Los titulares de los órganos que se relacionan en los párrafos a), b) c) y d) del apartado 1 de este artículo designarán a los funcionarios y funcionarias habilitados para la emisión de las copias electrónicas auténticas, que se llevará a cabo mediante el correspondiente proceso de digitalización.

Artículo 49. *Emisión de copias de documentos aportados en papel por el interesado.*

Cuando el interesado presente en papel una copia de un documento público administrativo o de un documento privado para incorporarlo a un expediente administrativo,

el proceso de digitalización por la Administración Pública generará una copia electrónica que tendrá el mismo valor que la copia presentada en papel.

Artículo 50. *Referencia temporal de los documentos administrativos electrónicos.*

1. Todos los documentos administrativos electrónicos deberán llevar asociadas una de las siguientes modalidades de referencia temporal, de acuerdo con lo que determinen las normas reguladoras de los respectivos procedimientos:

a) Marca de tiempo, entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

b) Sello electrónico cualificado de tiempo, entendiendo por tal la asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador cualificado de servicios de confianza que asegure la exactitud e integridad de la marca de tiempo del documento. Los sellos electrónicos de tiempo no cualificados serán asimilables a todos los efectos a las marcas de tiempo.

2. La marca de tiempo será utilizada en todos aquellos casos en los que las normas reguladoras no establezcan la utilización de un sello electrónico cualificado de tiempo

La información relativa a las marcas y sellos electrónicos cualificados de tiempo se asociará a los documentos electrónicos en la forma que determine el Esquema Nacional de Interoperabilidad y normativa correspondiente.

3. La relación de prestadores cualificados de servicios de confianza que prestan servicios de sellado de tiempo en el sector público deberá estar incluida en la «Lista de confianza de prestadores cualificados de servicios de confianza».

Artículo 51. *Configuración del expediente administrativo electrónico.*

1. El foliado de los expedientes administrativos electrónicos se llevará a cabo mediante un índice electrónico autenticado que garantizará la integridad del expediente y permitirá su recuperación siempre que sea preciso.

2. Un mismo documento electrónico podrá formar parte de distintos expedientes administrativos.

3. El índice electrónico autenticado será firmado por el titular del órgano que conforme el expediente para su tramitación o bien podrá ser sellado electrónicamente en el caso de expedientes electrónicos que se formen de manera automática, a través de un sistema que garantice su integridad.

Artículo 52. *Ejercicio del derecho de acceso al expediente electrónico y obtención de copias de los documentos electrónicos.*

De acuerdo con lo previsto en el artículo 53.1.a) de la Ley 39/2015, de 1 de octubre, el derecho de acceso de las personas interesadas que se relacionen electrónicamente con las Administraciones Públicas al expediente electrónico y, en su caso, a la obtención de copia total o parcial del mismo, se entenderá satisfecho mediante la puesta a disposición de dicho expediente en el Punto de Acceso General electrónico de la Administración competente o en la sede electrónica o sede electrónica asociada que corresponda.

A tal efecto, la Administración destinataria de la solicitud remitirá al interesado o, en su caso a su representante, la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición, garantizando aquella el acceso durante el tiempo que determine la correspondiente política de gestión de documentos electrónicos siempre de acuerdo con el dictamen de valoración emitido por la autoridad calificadora correspondiente, y el cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal y de transparencia y acceso a la información pública y de patrimonio documental, histórico y cultural.

Artículo 53. *Tiempo de conservación y destrucción de documentos.*

1. Los documentos presentados por el interesado en soporte papel que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez digitalizados serán conservados a su disposición durante seis meses para que pueda

recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

2. Los documentos presentados por el interesado en formato electrónico dentro de un dispositivo, que por cualquier circunstancia no le puedan ser devueltos en el momento de su presentación, una vez incorporados al expediente serán conservados a su disposición durante seis meses para que pueda recogerlos, independientemente del procedimiento administrativo al que se incorporen o de la Administración Pública a que vayan dirigidos, salvo que reglamentariamente la Administración correspondiente establezca un plazo mayor.

3. Transcurrido el plazo previsto en los apartados anteriores, la destrucción de los documentos se realizará de acuerdo con las competencias del Ministerio de Cultura y Deporte o del órgano competente de la comunidad autónoma, y siempre que no se trate de documentos con valor histórico, artístico u otro relevante o de documentos en los que la firma u otras expresiones manuscritas o mecánicas confieran al documento un valor especial.

4. Cuando la generación de copias electrónicas auténticas se realice a partir de documentos originales o copias auténticas de documentos en soporte no electrónico que se conserven formando parte de sus correspondientes expedientes y series documentales en cualesquiera de las oficinas, archivos o dependencias de cualquier organismo de las Administraciones públicas, dichos documentos originales o copias auténticas de documentos en soporte no electrónico se restituirán a sus oficinas, archivos o dependencias de origen, donde les será de aplicación la normativa específica en materia de archivos y conservación del patrimonio documental en su respectivo ámbito y siguiendo lo establecido por las autoridades calificadoras que correspondan.

5. En el ámbito estatal, se estará a lo preceptuado en el Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y entidades de derecho público y la conservación de documentos administrativos en soporte distinto al original.

CAPÍTULO II

Archivo electrónico de documentos

Artículo 54. *Conservación de documentos electrónicos.*

1. De acuerdo con lo previsto en el artículo 46 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, así como sus organismos públicos y entidades de derecho público vinculados o dependientes, deberán conservar en soporte electrónico todos los documentos que formen parte de un expediente administrativo y todos aquellos documentos con valor probatorio creados al margen de un procedimiento administrativo.

La copia electrónica auténtica generada conforme a lo dispuesto en el artículo 27 de la Ley 39/2015, de 1 de octubre, tiene la consideración de patrimonio documental a efectos de aplicación de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español o la normativa autonómica correspondiente, siendo el periodo de conservación de los documentos el establecido por las autoridades calificadoras que correspondan.

2. Cada Administración Pública, regulará los períodos mínimos de conservación de los documentos electrónicos, que formen parte del expediente de un procedimiento cuya tramitación haya concluido, conforme a su normativa específica de archivos y patrimonio documental.

Cuando se tenga conocimiento por la Administración Pública, organismo o entidad de la existencia de procedimientos judiciales que afecten o puedan afectar a documentos electrónicos, estos deberán conservarse a disposición de los órganos jurisdiccionales, hasta tanto exista constancia de la terminación del procedimiento judicial correspondiente en las sucesivas instancias, por haber recaído resolución no susceptible de recurso o procedimiento alguno ante órganos jurisdiccionales nacionales o internacionales.

3. La conservación de los documentos electrónicos deberá realizarse de forma que permita su acceso y comprenda, como mínimo, su identificación, contenido, metadatos, firma, estructura y formato.

También será posible la inclusión de su información en bases de datos siempre que, en este último caso, consten los criterios para la reconstrucción de los formularios o modelos electrónicos origen de los documentos, así como para la comprobación de la identificación o firma electrónica de dichos datos.

Los plazos de conservación de esta información están sujetos a los mismos plazos establecidos para los correspondientes documentos electrónicos.

4. Para asegurar la conservación, acceso y consulta de los documentos electrónicos archivados con independencia del tiempo transcurrido desde su emisión, se podrán trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones, de acuerdo con lo previsto en el artículo 27 de la Ley 39/2015, de 1 de octubre y en la normativa específica de archivos y patrimonio documental, histórico y cultural.

Asimismo, se planificarán las actuaciones de preservación digital que garanticen la conservación a largo plazo de los documentos digitales y permitan de esta forma dar cumplimiento a lo establecido en el párrafo anterior

5. En todo caso, bajo la supervisión de los responsables de la seguridad y de los responsables de la custodia y gestión del archivo electrónico y de los responsables de las unidades productoras de la documentación se establecerán los planes y se habilitarán los medios tecnológicos para la migración de los datos a otros formatos y soportes que permitan garantizar la autenticidad, integridad, disponibilidad, conservación y acceso al documento cuando el formato de los mismos deje de figurar entre los admitidos por el Esquema Nacional de Interoperabilidad y normativa correspondiente.

Artículo 55. *Archivo electrónico único.*

1. El archivo electrónico único de cada Administración es el conjunto de sistemas y servicios que sustenta la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos administrativos o actuaciones correspondientes.

2. En el archivo electrónico único de la Administración General del Estado serán accesibles todos los documentos y expedientes electrónicos del sector público estatal una vez finalizados los procedimientos y en los plazos determinados por la Comisión Superior Calificadora de Documentos Administrativos de acuerdo con lo que se desarrolle reglamentariamente.

La gestión del archivo electrónico único garantizará la autenticidad, conservación, integridad, confidencialidad, disponibilidad y cadena de custodia de los expedientes y documentos almacenados, así como su acceso, en las condiciones exigidas por el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad, por la normativa de transparencia, acceso a la información pública y buen gobierno, por la legislación de archivos y patrimonio histórico y cultural y por la normativa específica que sea de aplicación, de acuerdo con lo que se desarrolle reglamentariamente.

TÍTULO IV

De las relaciones y colaboración entre las Administraciones Públicas para el funcionamiento del sector público por medios electrónicos

CAPÍTULO I

Colaboración entre las Administraciones Públicas para la actuación administrativa por medios electrónicos

Artículo 56. *Relaciones interadministrativas e interorgánicas por medios electrónicos.*

De acuerdo con lo previsto en el artículo 3.2 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas, en el ejercicio de sus competencias, estarán obligadas a

relacionarse a través de medios electrónicos entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

Artículo 57. *Comunicaciones en la Administración General del Estado.*

Los órganos de la Administración General del Estado y los organismos públicos y entidades de derecho público vinculados o dependientes de esta deberán utilizar medios electrónicos para comunicarse entre sí.

Las comunicaciones se efectuarán a través del Registro Electrónico General de la Administración General del Estado o registro del organismo público o entidad de derecho público de que se trate, o por cualquier otro medio electrónico que permita dejar constancia de su recepción.

Esta misma obligación será de aplicación a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando actúen en el ejercicio de potestades administrativas.

Artículo 58. *Adhesión a sedes electrónicas y sedes electrónicas asociadas.*

Las Administraciones Públicas y los organismos públicos y entidades de derecho público vinculados o dependientes podrán adherirse voluntariamente, mediante la formalización del correspondiente instrumento de adhesión, a las sedes electrónicas o sedes asociadas disponibles de titularidad de la misma Administración u otra Administración Pública, sin que se constituya como sede electrónica asociada.

Artículo 59. *Adhesión a la Carpeta Ciudadana del sector público estatal.*

Las Administraciones Públicas podrán integrar sus respectivas áreas personalizadas o carpetas ciudadanas a que se refiere el segundo párrafo del artículo 7.3 de este Reglamento, si las hubiere, o determinadas funcionalidades de las mismas, con la Carpeta Ciudadana prevista en el artículo 8 de este Reglamento, de forma que el interesado pueda acceder a sus contenidos o funcionalidades mediante procedimientos seguros que garanticen la integridad y confidencialidad de sus datos de carácter personal, independientemente de cuál haya sido su punto de acceso.

Artículo 60. *Sistema de interconexión de Registros.*

1. Las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de cada Administración, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán ser interoperables.

2. Las interconexiones entre Registros de las Administraciones Públicas deberán realizarse a través del Sistema de Interconexión de Registros (SIR) gestionado por el Ministerio de Asuntos Económicos y Transformación Digital en colaboración con el Ministerio de Política Territorial y Función Pública de acuerdo con lo previsto en el Esquema Nacional de Interoperabilidad y en la correspondiente Norma Técnica.

3. En el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de la Administración General del Estado, así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, deberán permitir la interoperabilidad con los sistemas de gestión de expedientes de las unidades de tramitación correspondientes.

Artículo 61. *Transmisiones de datos.*

1. Las transmisiones de datos a las que se refiere el artículo 155 de la Ley 40/2015, de 1 de octubre, realizadas a través de redes corporativas de las Administraciones Públicas para el envío de documentos elaborados por cualquier Administración, mediante consulta a las

plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, tienen la consideración de certificados administrativos necesarios para el procedimiento o actuación administrativa.

2. Cuando las personas interesadas no aporten datos y/o documentos que ya obren en poder de las Administraciones Públicas, de conformidad con lo establecido en la Ley 39/2015, de 1 de octubre, se seguirán las siguientes reglas:

a) Si el órgano administrativo encargado de la tramitación del procedimiento, puede acceder electrónicamente a los datos, documentos o certificados necesarios mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, los incorporará al procedimiento administrativo correspondiente. Quedará constancia en los ficheros del órgano, organismo público o entidad de derecho público cedente del acceso a los datos o documentos efectuado por el órgano u organismo cesionario.

b) Excepcionalmente, en caso de que no se pueda realizar el acceso electrónico a los datos mediante la consulta a que se refiere la letra anterior, se podrá solicitar por otros medios habilitados al efecto y se conservará la documentación acreditativa de la circunstancia que imposibilitó dicho acceso electrónico, incorporándola al expediente.

3. Toda transmisión de datos se efectuará a solicitud del órgano o entidad tramitadora en la que se identificarán los datos requeridos y sus titulares, así como la finalidad para la que se requieren. Además, si en la petición de datos interviene un empleado o empleada público se incluirá la identificación de este en la petición.

4. El órgano, organismo público o entidad de derecho público cesionario será responsable del correcto acceso electrónico a los datos cuya titularidad corresponda a otro órgano, organismo público o entidad de derecho público, así como de su utilización, en particular, cuando los datos a los que se accede tengan un régimen de especial protección. Asimismo, cuando para dicho acceso se requiera el consentimiento del interesado, el cesionario será responsable del requerimiento de dicho consentimiento.

5. La cesión de datos dentro de una actuación administrativa podrá llevarse a cabo, entre otras formas, de manera automatizada, entendiéndose por tal la consulta realizada íntegramente a través de medios telemáticos en la que no haya intervenido de forma directa un empleado o empleada público.

6. Las transmisiones de datos que se realicen en virtud del artículo 14 del Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) n.º 1024/2012 no requerirán previsualización de los datos por parte del usuario o usuaria solicitante para proceder a su uso por parte del órgano o entidad tramitadora.

Artículo 62. *Plataformas de intermediación de datos.*

1. Las plataformas de intermediación de datos dejarán constancia de la fecha y hora en que se produjo la transmisión, así como del procedimiento administrativo, trámite o actuación al que se refiere la consulta. Las plataformas de intermediación, o sistema electrónico equivalente, existentes en el sector público deberán ser interoperables con la Plataforma de Intermediación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes y entre ellas.

La adhesión a las plataformas de intermediación de datos requerirá que se garantice el cumplimiento de las condiciones de seguridad exigidas por los cedentes de la información para el tratamiento de datos por parte de la plataforma encargada del tratamiento de dichos datos y de los cesionarios de los mismos.

2. En el ámbito estatal, se dispondrá de la Plataforma de Intermediación de Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes a que se refiere la Ley 39/2015, de 1 de octubre. Dicha Plataforma será gestionada la Secretaría General de Administración Digital y actuará como un punto a través del cual cualquier órgano, organismo público o entidad de derecho público podrá consultar los datos o documentos asociados al procedimiento de que se trate, con

independencia de que la presentación de los citados datos o documentos tenga carácter preceptivo o facultativo en el procedimiento de que se trate.

3. La Plataforma de Intermediación de la Administración General del Estado actuará como punto de conexión con el sistema técnico regulado por el Reglamento (UE) n.º 2018/1724 del Parlamento Europeo y del Consejo, de 2 de octubre de 2018, para el intercambio automático de datos o documentos a nivel europeo.

Artículo 63. *Remisión electrónica de expedientes administrativos en el ámbito de las Administraciones públicas mediante puesta a disposición.*

1. Cuando desde una Administración Pública se solicite a otra un expediente electrónico, la remisión por esta, a través de un nodo de interoperabilidad, de la dirección electrónica o localizador que dé acceso al expediente electrónico puesto a disposición de la primera equivaldrá a la remisión del mismo, siempre que se garantice la integridad del acceso a lo largo del tiempo que determine la correspondiente política de gestión de documentos electrónicos y el cumplimiento de la normativa de interoperabilidad aplicable al tipo de expediente.

2. El mismo procedimiento previsto en el apartado anterior se podrá utilizar cuando la solicitud se produzca dentro del ámbito de una misma Administración Pública.

CAPÍTULO II

Transferencia y uso compartido de tecnologías entre Administraciones Públicas

Artículo 64. *Reutilización de sistemas y aplicaciones de las Administraciones Públicas.*

1. De acuerdo con lo previsto en el artículo 157 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas pondrán a disposición de cualquiera de ellas que lo solicite las aplicaciones, desarrolladas por sus servicios o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, salvo que la información a la que estén asociadas sea objeto de especial protección por estar previsto en una norma. Las Administraciones cedentes y cesionarias podrán acordar la repercusión del coste de adquisición o fabricación de las aplicaciones cedidas.

2. A tal efecto, de acuerdo con lo previsto en el artículo 158 de la Ley 40/2015, de 1 de octubre, las Administraciones Públicas mantendrán directorios actualizados de aplicaciones para su libre reutilización en modo producto o en modo servicio, de conformidad con lo dispuesto en el Esquema Nacional de Interoperabilidad.

Estos directorios deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, con el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización previsto en el artículo 17 del Real Decreto 4/2010, de 8 de enero.

3. Las condiciones de licenciamiento de los sistemas y aplicaciones de las Administraciones públicas y el uso y funcionamiento de los directorios de aplicaciones reutilizables deberán ajustarse a lo previsto en el Real Decreto 4/2010, de 8 de enero.

4. Las Administraciones públicas procurarán la construcción de aplicaciones reutilizables, bien en modo producto o en modo servicio, con el fin de favorecer las actuaciones de compartir, reutilizar y colaborar, en beneficio de una mejor eficiencia y para atender de forma efectiva las solicitudes recibidas en virtud del artículo 157 de la Ley 40/2015, de 1 de octubre.

5. Las Administraciones Públicas, con carácter previo a la adquisición, desarrollo o al mantenimiento a lo largo de todo el ciclo de vida de una aplicación, tanto si se realiza con medios propios o por la contratación de los servicios correspondientes, deberán consultar en el Directorio general de aplicaciones de la Administración General del Estado para su libre reutilización, si existen soluciones disponibles para su reutilización, que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir, y siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

Las conclusiones con respecto al resultado de dicha consulta al directorio general se incorporarán en el expediente de contratación y reflejarán, en su caso, que no existen

soluciones disponibles para su reutilización que puedan satisfacer total o parcialmente las necesidades, mejoras o actualizaciones que se pretenden cubrir.

En el caso de existir una solución disponible para su reutilización total o parcial, la justificación de la no reutilización se realizará en términos de eficiencia conforme a lo establecido en el artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

Artículo 65. *Adhesión a las plataformas de la Administración General del Estado.*

1. La adhesión al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado prevista en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento, así como a aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en estas normas se realizará mediante adhesión por el órgano competente de la Administración Pública que corresponda, en el que se dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

A tal efecto, los modelos de adhesión a las plataformas, registros o servicios, que incluirán los términos de prestación del servicio y de la contribución al sostenimiento del mismo, se aprobarán mediante Resolución de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital o, en su caso, del órgano directivo, organismo público o entidad de derecho público que sea competente de las plataformas, registros o servicios de que se trate.

2. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación. Si la plataforma provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o de distinta plataforma, la autenticación de la entidad solicitante puede acreditarse, ante la entidad cedente, mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma en cuestión de la que es usuaria la entidad solicitante, que actuará en nombre de los órganos y organismos o entidades adheridos que actúan como solicitantes.

La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

3. Los órganos competentes para la gestión del procedimiento administrativo de las Administraciones que se adhieran a estas plataformas, registros o servicios electrónicos se responsabilizarán del uso que hagan de las mismas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de que una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, y sin perjuicio de la ampliación de plazos a que se refiere el artículo 32.4 de la Ley 39/2015, de 1 de octubre, cada Administración pública será responsable de la continuación de la tramitación de sus procedimientos administrativos y servicios a la ciudadanía.

4. La adhesión de las comunidades autónomas o entidades locales a las plataformas estatales o registros previstos en la disposición adicional segunda de la Ley 39/2015, de 1 de octubre, es voluntaria, si bien la no adhesión deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, para lo que se enviará el correspondiente informe al Ministerio de Asuntos Económicos y Transformación Digital, en el que deberá incluirse la justificación del cumplimiento de los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad y sus normas técnicas de desarrollo, de plataformas, registros o servicios electrónicos que se utilicen, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes plataformas.

Disposición adicional primera. *Obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado.*

Las personas participantes en procesos selectivos convocados por la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes a la misma, deberán realizar la presentación de las solicitudes y documentación y, en su caso, la subsanación y los procedimientos de impugnación de las actuaciones de estos procesos selectivos a través de medios electrónicos.

Disposición adicional segunda. *Formación de empleados y empleadas públicos de la Administración General del Estado.*

La Administración General del Estado promoverá la formación del personal a su servicio para garantizar el derecho de las personas interesadas a ser asistidas en el uso de medios electrónicos en sus relaciones con la Administración Pública, establecido en la Ley 39/2015, de 1 de octubre.

Disposición adicional tercera. *Nodo de interoperabilidad de identificación electrónica del Reino de España.*

1. Se crea el nodo de interoperabilidad de identificación electrónica del Reino de España para el reconocimiento mutuo de identidades electrónicas entre los Estados miembros, de acuerdo con lo previsto en el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.
2. El nodo de interoperabilidad de identificación electrónica del Reino de España se gestionará por el Ministerio de Asuntos Económicos y Transformación Digital.
3. Las entidades pertenecientes al sector público deberán definir y publicar en su sede electrónica el nivel de seguridad en la identificación electrónica exigido en los procedimientos y servicios que gestionan, de acuerdo con el Reglamento (UE) n.º 910/2014, de 23 de julio de 2014. Este nivel de seguridad en la identificación electrónica del sistema de información que soporta el procedimiento o servicio se determinará sobre la base del análisis de riesgos, de acuerdo con el Esquema Nacional de Seguridad y normativa correspondiente.
4. Las entidades pertenecientes al sector público deberán admitir en todo caso, en el acceso electrónico a sus procedimientos y servicios los esquemas de identificación notificados por otros Estados Miembros al amparo del Reglamento (UE) n.º 910/2014, de 23 de julio de 2014, siempre que se den estas dos condiciones:

a) El esquema de identificación utilizado tenga un nivel de seguridad en la identificación electrónica sustancial o alto.
b) El nivel de seguridad de dicho esquema sea igual o superior al nivel de seguridad exigido por el procedimiento o servicio de acuerdo con el apartado 3.

Disposición adicional cuarta. *Adhesión de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado en el ejercicio de potestades administrativas a las sedes electrónicas y sedes electrónicas asociadas y sistema de firma y notificaciones electrónicas aplicables.*

De acuerdo con lo previsto en el artículo 2.2.b) de la Ley 39/2015, de 1 de octubre, y el artículo 2.2.b) de la Ley 40/2015, de 1 de octubre, cuando las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado ejerzan potestades administrativas y, en consecuencia, les sea de aplicación este Reglamento, se observarán las siguientes disposiciones:

a) De acuerdo con lo previsto en el artículo 58, las entidades de derecho privado tendrán que adherirse a la sede electrónica asociada del ministerio con el que mantengan la vinculación o dependencia o, en su caso, a la sede electrónica o sede electrónica asociada del organismo de derecho público con el que mantengan la misma, en ambos casos mediante la formalización del correspondiente instrumento de adhesión.

Las personas interesadas obligadas a relacionarse electrónicamente con las entidades de derecho privado en el ejercicio de dichas potestades realizarán los trámites del procedimiento mediante los modelos normalizados que estarán disponibles en la sede electrónica asociada o, en su caso, sede electrónica a la que se haya adherido la entidad. El mismo régimen se aplicará a los sujetos no obligados que hayan optado por medios electrónicos de acuerdo con lo previsto en el artículo 3 de este Reglamento.

b) Según lo previsto en los artículos 20.2 y 22.4, mediante orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se determinarán reglamentariamente los medios admitidos para la firma electrónica en los procedimientos tramitados en el ejercicio de potestades administrativas por parte de las entidades de derecho privado vinculadas o dependientes de la Administración General del Estado.

c) De conformidad con lo previsto en el artículo 42, las notificaciones electrónicas que las entidades de derecho privado tengan que practicar se llevarán a cabo en la misma forma que el responsable de la sede electrónica asociada o sede electrónica a la que esté adherida la entidad haya dispuesto para sus propias notificaciones.

Disposición adicional quinta. *Adhesión de los órganos constitucionales al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado.*

1. Sin perjuicio de lo previsto en el artículo 65 de este Reglamento, los órganos constitucionales podrán adherirse al uso de las plataformas, registros o servicios electrónicos de la Administración General del Estado y aquellos otros que puedan facilitar el cumplimiento de lo dispuesto en la Ley 39/2015, de 1 de octubre, en la Ley 40/2015, de 1 de octubre, y en este Reglamento.

2. La adhesión se realizará mediante un acuerdo o acto de adhesión en el que la autoridad competente de las instituciones u órganos anteriores dejará constancia de la voluntad de este de adherirse a las plataformas, registros o servicios electrónicos y de aceptar en su integridad las condiciones de uso determinadas por el órgano titular de la plataforma o servicio, incluyendo el comienzo efectivo del mismo.

Para el estudio de su viabilidad, remitirá con carácter previo al Ministerio al que pertenezca el órgano titular de la plataforma o servicio una memoria justificativa y económica en que se explicite el volumen de trámites que estaría previsto realizar a través de la plataforma, el registro o servicio electrónico de que se trate, los efectos presupuestarios y económicos y cualquier otra razón de interés general que justifique su adhesión.

3. La adhesión a una plataforma, registro o servicio electrónico de la Administración General del Estado no supondrá un cambio de la titularidad sobre las actuaciones administrativas realizadas en el procedimiento administrativo de que se trate, que corresponderá a la Administración competente para su tramitación.

Si la plataforma, registro o servicio electrónico provee un servicio que requiere el intercambio de información entre dos entidades usuarias de la misma o distinta plataforma, la autenticación de la entidad solicitante puede acreditarse ante la entidad cedente mediante un sello electrónico cualificado del órgano, organismo público o entidad de derecho público que gestiona la plataforma.

4. La adhesión a una plataforma de la Administración General del Estado requerirá que se cumplan las condiciones de seguridad exigidas por los cedentes de la información.

5. Los órganos competentes en las instituciones u órganos adheridos se responsabilizarán del uso que hagan de las plataformas en el ejercicio de sus competencias, correspondiendo al órgano responsable de la plataforma su gestión y mantenimiento. En el supuesto de una incidencia técnica imposibilite el funcionamiento ordinario del sistema o aplicación que corresponda, los órganos competentes en las instituciones u órganos adheridos serán responsables de la continuación de la tramitación de sus procedimientos administrativos.

Disposición adicional sexta. *Situación de las sedes electrónicas y subsedes electrónicas en el ámbito estatal existentes a la entrada en vigor de este real decreto.*

1. En aplicación de lo previsto en el artículo 38 de la Ley 40/2015, de 1 de octubre, las sedes electrónicas existentes en la Administración General del Estado en la fecha de entrada en vigor de este real decreto pasan a tener naturaleza de sedes electrónicas

asociadas de la sede electrónica de la Administración General del Estado, que es la sede del Punto de Acceso General electrónico (PAGe) de la Administración General del Estado, sin necesidad de modificar su instrumento de creación. Las subsedes electrónicas existentes en la fecha de entrada en vigor de este real decreto pasarán también a tener naturaleza de sedes electrónicas asociadas.

2. Las sedes electrónicas de los organismos públicos o entidades de derecho público vinculados o dependientes existentes en la fecha de entrada en vigor de este real decreto mantendrán su naturaleza de sede electrónica. Las subsedes electrónicas de estos pasarán a tener naturaleza de sedes electrónicas asociadas.

Disposición adicional séptima. *Interoperabilidad de los registros electrónicos de apoderamientos.*

1. En aplicación de lo previsto en el artículo 6 de la Ley 39/2015, de 1 de octubre, y el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, la Norma Técnica de Interoperabilidad establecerá el modelo de datos y las condiciones de interoperabilidad de los registros electrónicos de apoderamientos, abordando los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, a los registros mercantiles, de la propiedad y a los protocolos notariales.

2. En el ámbito de la Administración General del Estado, el cumplimiento de las previsiones del artículo 33.2 del Reglamento sobre el acceso al Registro Electrónico de Apoderamientos de la Administración General del Estado está vinculado a la aprobación y aplicación de la Norma Técnica a que se refiere el apartado 1 anterior.

Disposición adicional octava. *Supletoriedad en Registro Civil.*

De conformidad con lo dispuesto en el artículo 88 y en la Disposición final primera de la Ley 20/2011, de 21 de julio, del Registro Civil, este Reglamento será de aplicación supletoria en lo no previsto en dicha Ley y su normativa de desarrollo específica, en cuanto a todo lo relacionado con la tramitación administrativa de los procedimientos específicos de Registro Civil.

Disposición adicional novena. *Autorización de los sistemas de identificación previstos en el artículo 9.2.c) y de los sistemas de firma previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre.*

1. Los sistemas de identificación a que se refiere el artículo 9.2.c) y los sistemas de firma a que se refiere el artículo 10.2.c) de la ley 39/2015, de 1 de octubre, que, en ambos casos, se hubieran puesto en servicio hasta el 6 de noviembre de 2019, fecha de entrada en vigor de la modificación de dichos artículos en virtud del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, no requerirán la autorización de la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, previo informe vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior, siempre y cuando no hayan sido modificados tras dicha fecha.

2. Los sistemas que, tras el 6 de noviembre de 2019, hayan sido autorizados en aplicación de las previsiones de los artículos 9.2.c) y 10.2.c) de la Ley 39/2015, de 1 de octubre, y sean modificados posteriormente, deberán ser objeto de una nueva autorización previa a su puesta en servicio.

Disposición adicional décima. *Especialidades por razón de materia.*

1. De acuerdo con la disposición adicional primera de la Ley 39/2015, de 1 de octubre, los procedimientos administrativos regulados en leyes especiales por razón de la materia que no exijan alguno de los trámites previstos en la citada ley o regulen trámites adicionales o distintos se regirán, respecto a estos, por lo dispuesto en dichas leyes especiales.

2. Las siguientes actuaciones y procedimientos se regirán por su normativa específica y supletoriamente por lo dispuesto en la Ley 39/2015, de 1 de octubre:

a) Las actuaciones y procedimientos de aplicación de los tributos en materia tributaria y aduanera, así como su revisión en vía administrativa.

b) Las actuaciones y procedimientos de gestión, inspección, liquidación, recaudación, impugnación y revisión en materia de Seguridad Social y desempleo.

c) Las actuaciones y procedimientos sancionadores en materia tributaria y aduanera, en el orden social, en materia de tráfico y seguridad vial y en materia de extranjería.

d) Las actuaciones y procedimientos en materia de extranjería y asilo.

3. De acuerdo con lo previsto en la Disposición adicional decimoséptima de la Ley 40/2015, de 1 de octubre, la Agencia Estatal de Administración Tributaria se regirá por su legislación específica y únicamente de forma supletoria y en tanto resulte compatible con su legislación específica por lo previsto en dicha Ley. El acceso, la cesión o la comunicación de información de naturaleza tributaria se regirán en todo caso por su legislación específica.

ANEXO

Definiciones

– Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otras personas usuarias.

– Archivo electrónico único de cada Administración: Conjunto de sistemas y servicios que sustente la gestión, custodia y recuperación de los documentos y expedientes electrónicos así como de otras agrupaciones documentales o de información una vez finalizados los procedimientos o actuaciones correspondientes.

– Autenticación: Procedimiento de verificación de la identidad digital de un sujeto en sus interacciones en el ámbito digital, típicamente mediante factores tales como «algo que se sabe»(contraseñas o claves concertadas), «algo que se tiene» sean componentes lógicos (como certificados software) o dispositivos físicos (en expresión inglesa, tokens), o «algo que se es» (elementos biométricos), factores utilizados de manera aislada o combinados.

– Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Canal: Estructura o medio de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, etc.).

– Certificado electrónico: Documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con su propietario. Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

– Certificado cualificado: Un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

– Certificado cualificado de sello electrónico: Certificado de sello electrónico que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo III del Reglamento UE 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones, electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE

– Código malicioso: Tipo de software de carácter dañino que crea o aprovecha vulnerabilidades en dispositivos, sistemas y archivos informáticos que permiten el acceso remoto no autorizado, la generación de puertas traseras, el robo o exfiltración de datos, la destrucción de información, u otras acciones perjudiciales.

– Código Seguro de Verificación (CSV): Código que identifica a un documento electrónico y cuya finalidad es garantizar el origen e integridad de los documentos mediante

el acceso a la sede electrónica correspondiente; el carácter único del código generado para cada documento; su vinculación con el documento generado, de forma que cualquier modificación del documento generado dará lugar a un nuevo documento con un código seguro de verificación diferente; la posibilidad de verificar el documento en la sede electrónica como mínimo por el tiempo que se establezca en la resolución que autorice la aplicación de este procedimiento; así como un acceso al documento restringido a quien disponga del código seguro de verificación.

– Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Copia auténtica: Tendrá la consideración de copia auténtica de un documento público administrativo o privado original o de otra copia auténtica, la realizada, cualquiera que sea su soporte, por los órganos competentes de las Administraciones Públicas en las que quede garantizada la identidad del órgano que ha realizado la copia y su contenido

– Copia autorizada electrónica: documento notarial electrónico generado por el notario que autorizó la escritura, con el mismo valor y efectos que la copia en papel y al cual se le atribuye también valor de documento público.

– Digitalización: Proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

– Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones

– Directorio de aplicaciones reutilizables: instrumento que contiene la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

– Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

– Entorno cerrado de comunicación: escenario de comunicaciones delimitado, controlado y protegido en el que los participantes se relacionan a través de medios electrónicos, según unas garantías y condiciones determinadas que incluyen la relación de emisores y receptores autorizados, la naturaleza de los datos a intercambiar y las medidas de seguridad y protección de datos.

– Especificación técnica: Según el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea, documento en el que se prescriben los requisitos técnicos que debe reunir un producto, proceso, servicio o sistema y que establece uno o más de los aspectos siguientes:

• Las características que debe tener un producto, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud y seguridad y sus dimensiones, así como los requisitos aplicables al producto en lo que respecta a la denominación con la que se vende, la terminología, los símbolos, los ensayos y los métodos de ensayo, el embalaje, el marcado o el etiquetado y los procedimientos de evaluación de la conformidad;

• los métodos y procedimientos de producción de los productos agrícolas, definidos en el artículo 38, apartado 1, del TFUE, de los productos destinados a la alimentación humana y animal y de los medicamentos, así como los métodos y procedimientos de producción relacionados con los demás productos, en caso de que estos influyan en sus características;

• las características que debe tener un servicio, como los niveles de calidad, rendimiento, interoperabilidad, protección del medio ambiente, salud o seguridad, así como los requisitos aplicables al proveedor en lo que respecta a la información que debe facilitarse a la persona destinataria, tal como se especifica en el artículo 22, apartados 1 a 3, de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior.

• los métodos y los criterios para evaluar el rendimiento de los productos de construcción, tal como se definen en el artículo 2, punto 1, del Reglamento (UE) n.º 305/2011

del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, por el que se establecen condiciones armonizadas para la comercialización de productos de construcción, en relación con sus características esenciales.

– Esquema Nacional de Interoperabilidad: Instrumento que comprende el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

– Esquema Nacional de Seguridad: Instrumento que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

– Expediente administrativo: Conjunto ordenado de documentos y actuaciones relativos a la resolución administrativa, así como las diligencias encaminadas a ejecutarla.

– Firma electrónica: Los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: La firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento eIDAS.

– Firma electrónica cualificada: Una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Formato de documento: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria. Se corresponde habitualmente con una especificación técnica.

– Identificación: Procedimiento para reconocer de forma única la identidad de un sujeto que culmina tras un registro previo con la asignación de un elemento identificador singular en formato electrónico que representa de forma única a una persona física o jurídica o a una persona física que representa a una persona jurídica para interacción en el entorno digital.

– Infraestructura o servicio común: Capacidad organizativa y técnica que satisface necesidades comunes de las personas usuarias en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

– Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que estos dan soporte, de compartir datos y posibilitar el intercambio de información entre ellos.

– Licenciamiento: Condiciones aplicables a la reutilización de cualquier tipo de material en formato electrónico que pueda ser empleado de forma recurrente.

– Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

– Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

– Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

– Nodo de interoperabilidad: Entidad que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que estas fijen.

– Política de firma electrónica: Conjunto de directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

– Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

– Portal de internet de una Administración Pública: Se entiende por portal de internet el punto de acceso electrónico cuya titularidad corresponda a una Administración Pública, organismo público o entidad de derecho público que permite el acceso a través de internet a la información publicada y, en su caso, a la sede electrónica correspondiente.

– Prestador de Servicios de Confianza: Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza, según lo previsto en el Reglamento eIDAS.

– Punto de Acceso General: Portal de internet que facilita el acceso a los servicios, trámites e información de los órganos, organismos públicos y entidades vinculados o dependientes de la Administración Pública correspondiente y aglutina o conduce a las sedes electrónicas asociadas de sus órganos y las sedes electrónicas de sus organismos públicos y entidades de derecho público.

– Sello electrónico: Datos en formato electrónico anejos a otros datos en formato electrónico, o asociados de manera lógica con ellos, para garantizar el origen y la integridad de estos últimos.

– Sello electrónico avanzado: Sello electrónico que cumple los siguientes requisitos: 1) estar vinculado al creador del sello de manera única; 2) permitir la identificación del creador del sello; 3) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control, y 4) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

– Sello electrónico cualificado: Sello electrónico avanzado que se crea mediante un dispositivo cualificado de creación de sellos electrónicos y que se basa en un certificado cualificado de sello electrónico.

– Sede electrónica: Dirección electrónica, disponible para la ciudadanía a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a uno o varios organismos públicos o entidades de derecho público en el ejercicio de sus competencias.

– Sede electrónica asociada: Sede electrónica disponible para la ciudadanía a través de redes de telecomunicaciones que se crea por razones organizativas o técnicas vinculada a la sede electrónica de una Administración Pública o a la sede electrónica de un organismo público o entidad de derecho público.

– Sello de tiempo: Asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento

– Sistema de Interconexión de Registros: Infraestructura básica que permite el intercambio de asientos electrónicos de registro entre las Administraciones Públicas.

– Trazabilidad: Posibilidad de identificar el origen de un documento en las distintas fases de su producción, pudiendo determinar en qué fase y por quién se han producido, en su caso, las modificaciones del documento original.

§ 5

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems)*», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

Artículo 3. *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Artículo 4. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de términos incluido en el anexo IV.

CAPÍTULO II

Principios básicos

Artículo 5. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades.

Artículo 6. *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Artículo 7. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

5. Sin merma de los restantes principios básicos y requisitos mínimos establecidos, el sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 9. *Existencia de líneas de defensa.*

1. El sistema de información ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas sea comprometida, permita:

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 10. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 11. *Diferenciación de responsabilidades.*

1. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio, el responsable de la seguridad y el responsable del sistema.

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

3. La política de seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad

Artículo 12. *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

a) Los objetivos o misión de la organización.

b) El marco regulatorio en el que se desarrollarán las actividades.

c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.

d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad y la relación con otros elementos de la organización.

e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.

4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.

5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

Artículo 13. *Organización e implantación del proceso de seguridad.*

1. La seguridad de los sistemas de información deberá comprometer a todos los miembros de la organización.
2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

a) El responsable de la información determinará los requisitos de la información tratada
b) El responsable del servicio determinará los requisitos de los servicios prestados.
c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.
4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.
5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Artículo 14. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.
3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Artículo 15. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.
2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Artículo 16. *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.
2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Artículo 17. *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 18. *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Artículo 19. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Artículo 20. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 21. *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.
2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 22. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.
2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.
3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 23. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Artículo 24. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Artículo 25. *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 26. *Continuidad de la actividad.*

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Artículo 27. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Artículo 28. *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

a) Los activos que constituyen los sistemas de información concernidos.
b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

Artículo 29. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

Artículo 30. *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

Seguridad de los sistemas: auditoría, informe e incidentes de seguridad

Artículo 31. *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurran impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

Artículo 32. *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

Artículo 33. *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response Team),* que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team,* en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

Artículo 34. *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

CAPÍTULO V

Normas de conformidad

Artículo 35. *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

2. El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Artículo 36. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 37. *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

Artículo 38. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoria de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

CAPÍTULO VI

Actualización del Esquema Nacional de Seguridad

Artículo 39. *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

CAPÍTULO VII

Categorización de los sistemas de información

Artículo 40. *Categorías de seguridad.*

1. La categoría de seguridad de un sistema de información modulará el equilibrio entre la importancia de la información que maneja y los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

Artículo 41. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

Disposición adicional primera. *Formación.*

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

Disposición adicional segunda. *Desarrollo del Esquema Nacional de Seguridad.*

En desarrollo de lo dispuesto en este real decreto, la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de dicha Secretaría de Estado.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

Disposición adicional tercera. *Respeto del principio de «no causar un perjuicio significativo» al medioambiente.*

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm)* y las condiciones del etiquetado climático y digital.

Disposición transitoria única. *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.ª, 149.1.21.ª y 149.1.29.ª de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

Disposición final segunda. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

Este real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Categorías de seguridad de los sistemas de información

1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

a) Confidencialidad [C].
b) Integridad [I].
c) Trazabilidad [T].
d) Autenticidad [A].
e) Disponibilidad [D].

3. Determinación del nivel de seguridad requerido en una dimensión de seguridad

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada dimensión de seguridad afectada se adscribirá a uno de los siguientes niveles de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño menor en los activos de la organización.
3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4.º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio grave:

1.º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
2.º Causar un daño significativo en los activos de la organización.
3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se aplicará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio muy grave:

1.º La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
2.º Causar un daño muy grave, e incluso irreparable, de los activos de la organización.
3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Cuando un sistema de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de seguridad de un sistema de información

1. Se definen tres categorías de seguridad: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad ALTO.
b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad superior.
c) Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

2. La determinación de la categoría de seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

5. Secuencia de actuaciones para determinar la categoría de seguridad de un sistema

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

ANEXO II

Medidas de Seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría de seguridad del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

1. Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

a) Identificación de los tipos de activos presentes.
b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	**Marco organizativo**				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	**Marco operacional**				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

3. Marco organizativo [ORG]

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

– [org.1.1] Los objetivos o misión de la organización.
– [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
– [org.1.3] Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
– [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
– [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

– Categoría BÁSICA: org.1.
– Categoría MEDIA: org.1.
– Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que describan:

– [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
– [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: org.2.
– Categoría MEDIA: org.2.
– Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

– [org.3.1] Cómo llevar a cabo las tareas habituales.
– [org.3.2] Quién debe hacer cada tarea.
– [org.3.3] Cómo identificar y reportar comportamientos anómalos.
– [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.
f) Cualquier otra actividad relacionada con dicha información.

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

– Categoría BÁSICA: org.3.
– Categoría MEDIA: org.3.
– Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

– [org.4.1] Utilización de instalaciones, habituales y alternativas.
– [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
– [org.4.3] Entrada de aplicaciones en producción.
– [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
– [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
– [org.4.6] Utilización de soportes de información.
– [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
– [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

– Categoría BÁSICA: org.4.
– Categoría MEDIA: org.4.
– Categoría ALTA: org.4.

4. Marco operacional [op]

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R2

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

– [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
– [op.pl.1.2] Identifique las amenazas más probables.
– [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

– [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r1.2] Cuantifique las amenazas más probables.
– [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
– [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

– [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
– [op.pl.1.r2.2] Cuantifique las amenazas posibles.
– [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
– [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.1.
– Categoría MEDIA: op.pl.1 + R1.
– Categoría ALTA: op.pl.1 + R2.

4.1.2 Arquitectura de seguridad [op.pl.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

– [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
– [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
– [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.2.
– Categoría MEDIA: op.pl.2 + R1.
– Categoría ALTA: op.pl.2 + R1 + R2 + R3.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

– [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
– [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
– [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

– Categoría BÁSICA: op.pl.3.
– Categoría MEDIA: op.pl.3.
– Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

Con carácter previo a la puesta en explotación, se realizará un estudio que cubrirá los siguientes aspectos:

– [op.pl.4.1] Necesidades de procesamiento.
– [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
– [op.pl.4.3] Necesidades de comunicación.
– [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
– [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

– [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
– [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

– Nivel BAJO: op.pl.4.
– Nivel MEDIO: op.pl.4 + R1.
– Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.
En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.
Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.
– [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.pl.5.
– Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.
Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.
Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se

acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	T A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó da orden en sentido contrario.

c) Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará «periodo de retención».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.
– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

– Nivel BAJO: op.acc.1.
– Nivel MEDIO: op.acc.1 +R1.
– Nivel ALTO: op.acc.1+ R1.

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	+ R1

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
– [op.acc.2.2] Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.
– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.2.
– Nivel MEDIO: op.acc.2.
– Nivel ALTO: op.acc.2+ R1.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado pueda abusar de sus derechos para cometer alguna acción ilícita o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.
– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

Refuerzo R1-Segregación rigurosa.

– [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema.
– [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

– [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

– [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.acc.3.
– Nivel ALTO: op.acc.3 + R1.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

Los derechos de acceso de cada entidad, usuario o proceso se limitarán atendiendo a los siguientes principios:

– [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
– [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
– [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
– [op.acc.4.4] Capacidad de autorizar: Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.
– [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

Nivel BAJO: op.acc.4.
Nivel MEDIO: op.acc.4.
Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.
Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A

nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Requisitos.

– [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.

– [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

– [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.

– [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

– [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

– [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

– [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].
– Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.
– Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.
– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.
– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentican termina su relación con el sistema.
– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).
– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.
– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.
– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.
b) El tráfico deberá ser cifrado.

c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.
d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.6 + [R1 o R2 o R3 o R4] + R8 + R9.
– Nivel MEDIO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R8 + R9.
– Nivel ALTO: op.acc.6 + [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

– [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

– [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

– [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

– Categoría BÁSICA: op.exp.1.
– Categoría MEDIA: op.exp.1.
– Categoría ALTA: op.exp.1.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se configurarán los equipos previamente a su entrada en operación, de forma que:

– [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
– [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.
b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.
c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.
– Categoría MEDIA: op.exp.2.
– Categoría ALTA: op.exp.2.

4.3.3 Gestión de la configuración de seguridad [op.exp.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

Se gestionará de forma continua la configuración de los componentes del sistema, de forma que:

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).
– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).
– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).
– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).
– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).
– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.
– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.
– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.
– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.3.
– Categoría MEDIA: op.exp.3 + R1.
– Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

– [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
– [op.exp.4.2] Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la implantación o no de la actualización.
– [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).
3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.4.
– Categoría MEDIA: op.exp.4 + R1.
– Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

Se mantendrá un control continuo de los cambios realizados en el sistema, de forma que:

– [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.
– [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.
– [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.
– [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.
– [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

– [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.
– [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.
– [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.exp.5.
– Categoría ALTA: op.exp.5+ R1.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+R1+R2+R3+R4

Requisitos.

– [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
– [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales.
– [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
– [op.exp.6.4] Las bases de datos de detección de código dañino permanecerán permanentemente actualizadas.
– [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Refuerzo R1-Escaneo periódico.

– [op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

Refuerzo R2-Revisión preventiva del sistema.

– [op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

Refuerzo R3 - Lista blanca.

– [op.exp.6.r3.1] Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

Refuerzo R4-Capacidad de respuesta en caso de incidente.

– [op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*).

Refuerzo R5-Configuración de la herramienta de detección de código dañino.

– [op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema en el arranque y cada vez que se conecte un dispositivo extraíble.
– [op.exp.6.r5.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.6.
– Categoría MEDIA: op.exp.6+ R1 + R2.
– Categoría ALTA: op.exp.6+ R1 + R2 + R3 + R4.

4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2+ R3

Requisitos.

– [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
– [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos; la Ley Orgánica 3/2018, de 5

de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en este real decreto.

Refuerzo R1-Notificación.

– [op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

Refuerzo R2 –Detección y Respuesta.

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

– [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
– [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
– [op.exp.7.r2.3] Informar del incidente a los responsables de la información y servicios afectados y de las actuaciones llevadas a cabo para su resolución.
– [op.exp.7.r2.4] Medidas para:

a) Prevenir que se repita el incidente.
b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

Refuerzo R3-Reconfiguración dinámica.

La reconfiguración dinámica del sistema persigue detener, desviar o limitar ataques, acotando los daños.
– [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.
– [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

Refuerzo R4-Prevención y Respuesta Automática.

– [op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, la segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.7.
– Categoría MEDIA: op.exp.7+ R1 + R2.
– Categoría ALTA: op.exp.7+ R1 + R2 + R3.

4.3.8 Registro de la actividad [op.exp.8].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

Requisitos.

Se registrarán las actividades en el sistema, de forma que:

– [op.exp.8.1] Se generará un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
– [op.exp.8.2] Se activarán los registros de actividad en los servidores.

Refuerzo R1-Revisión de los registros.

– [op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad, buscando patrones anormales.

Refuerzo R2-Sincronización del reloj del sistema.

– [op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

Refuerzo R3-Retención de registros.

– [op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

Refuerzo R4-Control de acceso.

– [op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad de los mismos, solamente podrán ser accedidos o eliminarse por personal debidamente autorizado.

Refuerzo R5-Revisión automática y correlación de eventos.

– [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
– [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: op.exp.8.
– Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4.
– Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5.

4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

– [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
– [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
– [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.9.
– Categoría MEDIA: op.exp.9.
– Categoría ALTA: op.exp.9.

4.3.10 Protección de claves criptográficas [op.exp.10].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [op.exp.10.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
– [op.exp.10.2] Los medios de generación estarán aislados de los medios de explotación.
– [op.exp.10.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Refuerzo R1-Algoritmos autorizados.

– [op.exp.10.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Protección avanzada de claves criptográficas.

– [op.exp.10.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.10.
– Categoría MEDIA: op.exp.10 + R1.
– Categoría ALTA: op.exp.10 + R1.

4.4 Recursos externos [op.ext].

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como «servicio mínimo admisible», así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.1.
– Categoría ALTA: op.ext.1.

4.4.2 Gestión diaria [op.ext.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

Se establecerá lo siguiente:

– [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
– [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.2.
– Categoría ALTA: op.ext.2.

4.4.3 Protección de la cadena de suministro [op.ext.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	n.a.	aplica

Requisitos.

– [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
– [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
– [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

Refuerzo R1-Plan de contingencia.

– [op.ext.3.r1.1] El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos.
– [op.ext.3.r1.2] Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

Refuerzo R2-Sistema de gestión de la seguridad.

– [op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

Refuerzo R3-Lista de componentes software.

– [op.ext.3.r3.1] Se mantendrá actualizado un registro formal que contenga los detalles y las relaciones de la cadena de suministro de los diversos componentes utilizados en la construcción de programas informáticos, acorde a lo especificado en [mp.sw.1.r5]. Esta lista será proporcionada por el proveedor de la aplicación, librería o producto suministrado.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: no aplica.
– Categoría ALTA: op.ext.3.

4.4.4 Interconexión de sistemas [op.ext.4].

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

– [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.
– [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

Refuerzo R1-Coordinación de actividades.

– [op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: op.ext.4.
– Categoría ALTA: op.ext.4 + R1.

4.5 Servicios en la nube [op.nub].

4.5.1 Protección de servicios en la nube [op.nub.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a Service, SaaS*), Plataforma como Servicio (*Platform as a Service, PaaS*) e Infraestructura como Servicio (*Infrastructure as a Service, IaaS*) definidas en las guías CCN-STIC que sean de aplicación.
– [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, los sistemas de información que los soportan deberán ser conformes con el ENS o cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:

a) Auditoría de pruebas de penetración (*pentesting*).
b) Transparencia.
c) Cifrado y gestión de claves.
d) Jurisdicción de los datos.

Refuerzo R1- Servicios certificados.

– [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.
– [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

Refuerzo R2-Guías de Configuración de Seguridad Específicas.

– [op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica, orientadas tanto al usuario como al proveedor.

Aplicación de la medida.

– Categoría BÁSICA: op.nub.1.
– Categoría MEDIA: op.nub.1 + R1.
– Categoría ALTA: op.nub.1+ R1 + R2.

4.6 Continuidad del servicio [op.cont].

4.6.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: op.cont.1.
– Nivel ALTO: op.cont.1.

4.6.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan contemplará los siguientes aspectos:

– [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
– [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
– [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
– [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
– [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

Refuerzo R1-Plan de emergencia y contingencia.

– [op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del análisis de Impacto, se determinarán los aspectos a cubrir.

Refuerzo R2-Comprobación de integridad.

– [op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del sistema operativo, del firmware y de los ficheros de configuración.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.2.

4.6.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

– [op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.3.

4.6.4 Medios alternativos [op.cont.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

– [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto, se cubrirán los siguientes elementos del sistema:

a) Servicios contratados a terceros.
b) Instalaciones alternativas.
c) Personal alternativo.
d) Equipamiento informático alternativo.
e) Medios de comunicación alternativos.

– [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.
– [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

Refuerzo R1-Automatización de la transición a medios alternativos.

– [op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: op.cont.4.

4.7 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

4.7.1 Detección de intrusión [op.mon.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

– [op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

Refuerzo R1-Detección basada en reglas.

– [op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

Refuerzo R2-Procedimientos de respuesta.

– [op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

Refuerzo R3-Acciones predeterminadas.

– [op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.1.
– Categoría MEDIA: op.mon.1 + R1.
– Categoría ALTA: op.mon.1+ R1 + R2.

4.7.2 Sistema de métricas [op.mon.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+ R1+R2

Requisitos.

– [op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

Refuerzo R1-Efectividad del sistema de gestión de incidentes.

– [op.mon.2.r1.1] Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.

Refuerzo R2-Eficiencia del sistema de gestión de la seguridad.

– [op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.2.
– Categoría MEDIA: op.mon.2 + R1+ R2.
– Categoría ALTA: op.mon.2 + R1 + R2.

4.7.3 Vigilancia [op.mon.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	+ R1+R2	+ R1+R2+R3+R4+R5+R6

Requisitos.

– [op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

Refuerzo R1-Correlación de eventos.

– [op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

Refuerzo R2-Análisis dinámico.

– [op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

Refuerzo R3-Ciberamenazas avanzadas.

– [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamientos anómalos.
– [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat, APT*) mediante la detección de anomalías significativas en el tráfico de la red.

Refuerzo R4-Observatorios digitales.

– [op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías que pudieran representar indicadores de amenaza en contenidos digitales.

Refuerzo R5-Minería de datos.

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

– [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.
– [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

Refuerzo R6-Inspecciones de seguridad.

Periódicamente, o tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas, se realizarán las siguientes inspecciones:

– [op.mon.3.r6.1] Verificación de configuración.
– [op.mon.3.r6.2] Análisis de vulnerabilidades.
– [op.mon.3.r6.3] Pruebas de penetración.

Refuerzo R7-Interconexiones.

– [op.mon.3.r7.1] En las interconexiones que lo requieran se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

Aplicación de la medida.

– Categoría BÁSICA: op.mon.3.
– Categoría MEDIA: op.mon.3 + R1 + R2.
– Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6.

5. Medidas de protección [mp]

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función.
– [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.1.
– Categoría MEDIA: mp.if.1.
– Categoría ALTA: mp.if.1.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.2.
– Categoría MEDIA: mp.if.2.
– Categoría ALTA: mp.if.2.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado, y, en especial, para asegurar:

– [mp.if.3.1] Las condiciones de temperatura y humedad.
– [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
– [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.3.
– Categoría MEDIA: mp.if.3.
– Categoría ALTA: mp.if.3.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

– [mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

Refuerzo R1-Suministro eléctrico de emergencia.

– [mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.4.
– Nivel MEDIO: mp.if.4 + R1.
– Nivel ALTO: mp.if.4 + R1.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: mp.if.5.
– Nivel MEDIO: mp.if.5.
– Nivel ALTO: mp.if.5.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.if.6.
– Nivel ALTO: mp.if.6.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

Aplicación de la medida.

– Categoría BÁSICA: mp.if.7.
– Categoría MEDIA: mp.if.7.
– Categoría ALTA: mp.if.7.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

– [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.
– [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

Refuerzo R1-Habilitación Personal de Seguridad.

– [mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.per.1.
– Categoría ALTA: mp.per.1.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Se informará a cada persona que trabaje en el sistema de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad, contemplando:

– [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
– [mp.per.2.2] Contemplando tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
– [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
– [mp.per.2.4] En caso de personal contratado a través de un tercero:

• [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
• [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

Refuerzo R1-Confirmación expresa.

– [mp.per.2.r1.1] Se ha de obtener la confirmación expresa de que los usuarios conocen las instrucciones de seguridad necesarias y obligatorias y su aceptación, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.2.
– Categoría MEDIA: mp.per.2 + R1.
– Categoría ALTA: mp.per.2 + R1.

5.2.3 Concienciación [mp.per.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

– [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
– [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
– [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.3.
– Categoría MEDIA: mp.per.3.
– Categoría ALTA: mp.per.3.

5.2.4 Formación [mp.per.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción ante incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.per.4.
– Categoría MEDIA: mp.per.4.
– Categoría ALTA: mp.per.4.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

– [mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

Refuerzo R1-Almacenamiento del material.

– [mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.1.
– Categoría MEDIA: mp.eq.1 + R1.
– Categoría ALTA: mp.eq.1 + R1.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

– [mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Refuerzo R1-Cierre de sesiones.

– [mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

Aplicación de la medida (por autenticidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.eq.2.
– Nivel ALTO: mp.eq.2 + R1.

5.3.3 Protección de dispositivos portátiles [mp.eq.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+R1+R2

Requisitos.

Los equipos (ordenadores portátiles, tabletas, etc.) que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

– [mp.eq.3.1] Se llevará un inventario de dispositivos portátiles junto con una identificación de la persona responsable de cada uno de ellos y un control regular de que está positivamente bajo su control.
– [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.

– [mp.eq.3.3] Cuando un dispositivo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

– [mp.eq.3.4] Se evitará, en la medida de lo posible, que el dispositivo portátil contenga claves de acceso remoto a la organización que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización u otras de naturaleza análoga.

Refuerzo R1– Cifrado del disco.

– [mp.eq.3.r1.1] Se protegerá el dispositivo portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel MEDIO.

Refuerzo R2– Entornos protegidos.

– [mp.eq.3.r2.1] El uso de dispositivos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado y a salvo de hurtos y miradas indiscretas.

Aplicación de la medida.

– Categoría BÁSICA: mp.eq.3.
– Categoría MEDIA: mp.eq.3.
– Categoría ALTA: mp.eq.3 + R1 + R2.

5.3.4 Otros dispositivos conectados a la red [mp.eq.4].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener en algún momento acceso a la información, tales como:

a) Dispositivos multifunción: impresoras, escáneres, etc.
b) Dispositivos multimedia: proyectores, altavoces inteligentes, etc.
c) Dispositivos internet de las cosas, en inglés *Internet of Things* (*IoT*).
d) Dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device* (BYOD).
e) Otros.

Requisitos.

– [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.

– [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información. (Ver [mp.si.5]).

Refuerzo R1-Productos certificados.

– [mp.eq.4.r1.1] Se usarán, cuando sea posible, productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2-Control de dispositivos conectados a la red.

– [mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.eq.4.
– Nivel MEDIO: mp.eq.4 + R1.
– Nivel ALTO: mp.eq.4+ R1.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.com.1.1] Se dispondrá de un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
– [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

Aplicación de la medida.

– Categoría BÁSICA: mp.com.1.
– Categoría MEDIA: mp.com.1.
– Categoría ALTA: mp.com.1.

5.4.2 Protección de la confidencialidad [mp.com.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+R1+R2+R3

Requisitos.

– [mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R1-Algoritmos y parámetros autorizados.

– [mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R2-Dispositivos hardware.

– [mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R3-Productos certificados.

– [mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R4-Cifradores.

– [mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Refuerzo R5-Cifrado de información especialmente sensible.

– [mp.com.2.r5.1] Se cifrará toda la información transmitida.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.com.2.

– Nivel MEDIO: mp.com.2 + R1.
– Nivel ALTO: mp.com.2 + R1 + R2+ R3.

5.4.3 Protección de la integridad y de la autenticidad [mp.com.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

Requisitos.

– [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información. (Ver [op.acc.5]).
– [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

a) La alteración de la información en tránsito.
b) La inyección de información espuria.
c) El secuestro de la sesión por una tercera parte.

– [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico y en la normativa de aplicación.

Refuerzo R1-Redes privadas virtuales.

– [mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.com.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R3-Dispositivos hardware.

– [mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

Refuerzo R4-Productos certificados.

– [mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R5-Cifradores.

– [mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.com.3.
– Nivel MEDIO: mp.com.3 + R1 + R2.
– Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4.

5.4.4 Separación de flujos de información en la red [mp.com.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+[R1oR2oR3]	+[R2oR3]+R4

La segmentación acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.
Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

Requisitos.

Los flujos de información se separarán en segmentos de forma que:

– [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
– [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

Refuerzo R1-Segmentación lógica básica.

– [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (*Virtual Local Area Network, VLAN*).
– [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

• Usuarios.
• Servicios.
• Administración.

Refuerzo R2-Segmentación lógica avanzada.

– [mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network, VPN*).

Refuerzo R3-Segmentación física.

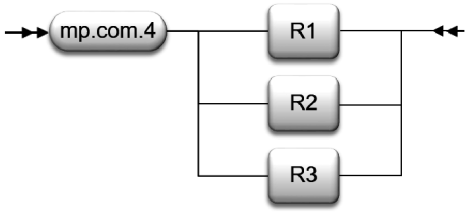
– [mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

Refuerzo R4-Puntos de interconexión.

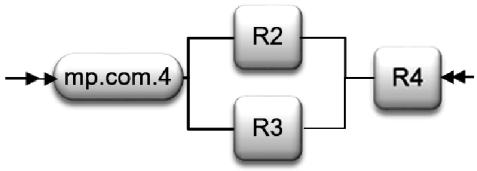
– [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
– [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado, (como en [mp.com.1]).

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.com.4+ [R1o R2 o R3].



– Categoría ALTA: mp.com.4+[R2 o R3] + R4.



5.5 Protección de los soportes de información [mp.si].

5.5.1 Marcado de soportes [mp.si.1].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos, contenidos multimedia -vídeos, cursos, presentaciones- etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

Refuerzo R1-Marca de agua digital.

– [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.
– [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia, etc.) podrán incluir una marca de agua según la política de seguridad.
– [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos, etc., presentarán una marca de agua en pantalla según la política de seguridad.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.1.
– Nivel ALTO: mp.si.1.

5.5.2 Criptografía [mp.si.2].

dimensiones	C I		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1 + R2

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB u otros de naturaleza análoga.

Requisitos.

– [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
– [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

Refuerzo R1– Productos certificados.

– [mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

Refuerzo R2-Copias de seguridad.

– [mp.si.2.r2.1] Las copias se seguridad se cifrarán utilizando algoritmos y parámetros autorizados por el CCN.

Aplicación de la medida (por confidencialidad e integridad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.si.2.
– Nivel ALTO: mp.si.2 + R1 + R2.

5.5.3 Custodia [mp.si.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

	aplica	aplica	aplica

Requisitos.

– [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
– [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

Aplicación de la medida.

– Categoría BÁSICA: mp.si.3.
– Categoría MEDIA: mp.si.3.
– Categoría ALTA: mp.si.3.

5.5.4 Transporte [mp.si.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

Requisitos.

– [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
– [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
– [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
– [mp.si.4.4] Se gestionarán las claves según [op.exp.10].

Aplicación de la medida.

– Categoría BÁSICA: mp.si.4.
– Categoría MEDIA: mp.si.4.
– Categoría ALTA: mp.si.4.

5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos y soportes susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Requisitos.

– [mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto del borrado seguro de su contenido que no permita su recuperación. Cuando la naturaleza del soporte no permita un borrado seguro, el soporte no podrá ser reutilizado en ningún otro sistema.

Las guías CCN-STIC del CCN precisarán los criterios para definir como seguro un mecanismo de borrado o de destrucción, en función de la sensibilidad de la información almacenada en el dispositivo.

Refuerzo R1-Productos certificados.

– [mp.si.5.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

Refuerzo R2 - Destrucción de soportes.

– [mp.si.5.r2.1] Una vez finalizado el ciclo de vida del soporte de información, deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.si.5.
– Nivel MEDIO: mp.si.5 + R1.
– Nivel ALTO: mp.si.5 + R1.

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	+R1+R2+R3+R4	+R1+R2+R3+R4

Requisitos.

– [mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

Refuerzo R1-Mínimo privilegio.

– [mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Refuerzo R2-Metodología de desarrollo seguro.

– [mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:

a) Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
b) Incluirá normas de programación segura, especialmente: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
c) Tratará específicamente los datos usados en pruebas.
d) Permitirá la inspección del código fuente.

Refuerzo R3-Seguridad desde el diseño.

– [mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:

a) Los mecanismos de identificación y autenticación.
b) Los mecanismos de protección de la información tratada.
c) La generación y tratamiento de pistas de auditoría.

Refuerzo R4-Datos de pruebas.

– [mp.sw.1.r4.1] Preferiblemente, las pruebas previas a la implantación o modificación de los sistemas de información no se realizarán con datos reales. En caso de que fuese necesario recurrir a datos reales se garantizará el nivel de seguridad correspondiente.

Refuerzo R5-Lista de componentes software.

– [mp.sw.1.r5.1] El desarrollador elaborará y mantendrá actualizada una relación formal de los componentes software de terceros empleados en la aplicación o producto. Se mantendrá un histórico de los componentes utilizados en las diferentes versiones del software. El contenido mínimo de la lista de componentes, que contendrá, al menos, la identificación del componente, el fabricante y la versión empleada, se concretará en una guía CCN-STIC del CCN.

Aplicación de la medida.

– Categoría BÁSICA: no aplica.
– Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4.
– Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R1

Requisitos.

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

– [mp.sw.2.1] Se comprobará que:

a) Se cumplen los criterios de aceptación en materia de seguridad.
b) No se deteriora la seguridad de otros componentes del servicio.

Refuerzo R1- Pruebas.

– [mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

Refuerzo R2-Inspección de código fuente.

– [mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

Aplicación de la medida.

– Categoría BÁSICA: mp.sw.2.
– Categoría MEDIA: mp.sw.2 + R1.
– Categoría ALTA: mp.sw.2 + R1.

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

– [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

– Categoría BÁSICA: mp.info.1.
– Categoría MEDIA: mp.info.1.
– Categoría ALTA: mp.info.1.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	aplica

Requisitos.

– [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
– [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
– [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 40 y los criterios generales señalados en el anexo I.
– [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
– [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.info.2.
– Nivel ALTO: mp.info.2.

5.7.3 Firma electrónica [mp.info.3].

dimensiones	I A		
nivel	BAJO	MEDIO	ALTO
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

Requisitos.

– [mp.info.3.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

Refuerzo R1-Certificados cualificados.

– [mp.info.3.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

Refuerzo R2-Algoritmos y parámetros autorizados.

– [mp.info.3.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo que resulte de aplicación.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

Refuerzo R3-Verificación y validación de firma.

– [mp.info.3.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

Refuerzo R4-Firma electrónica avanzada basada en certificados cualificados.

– [mp.info.3.r4.1] Se usará firma electrónica avanzada basada en certificados cualificados complementada por un segundo factor del tipo «algo que se sabe» o «algo que se es».

Refuerzo R5-Firma electrónica cualificada.

– [mp.info.3.r5.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

Aplicación de la medida (por integridad y autenticidad).

– Nivel BAJO: mp.info.3.
– Nivel MEDIO: mp.info.3 + R1 + R2 + R3.
– Nivel ALTO: mp.info.3 + R1 + R2 + R3 + R4.

5.7.4 Sellos de tiempo [mp.info.4].

dimensiones	T		
nivel	BAJO	MEDIO	ALTO
	n.a.	n.a.	aplica

Requisitos.

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

– [mp.info.4.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
– [mp.info.4.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
– [mp.info.4.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
– [mp.info.4.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) n.º 910/2014 y normativa de desarrollo.

Refuerzo R1-Productos certificados.

– [mp.info.4.r1.1.] Se utilizarán productos certificados según [op.pl.5].
– [mp.info.4.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la guía CCN-STIC Criptología de empleo en el ENS.

Aplicación de la medida (por trazabilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: no aplica.
– Nivel ALTO: mp.info.4.

5.7.5 Limpieza de documentos [mp.info.5].

dimensiones	C		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

– [mp.info.5.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Aplicación de la medida (por confidencialidad).

– Nivel BAJO: mp.info.5.
– Nivel MEDIO: mp.info.5.
– Nivel ALTO: mp.info.5.

5.7.6 Copias de seguridad [mp.info.6].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1 + R2

Requisitos.

– [mp.info.6.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa interna de la organización relativa a copias de seguridad.
– [mp.info.6.2] Los procedimientos de respaldo establecidos indicarán:

a) Frecuencia de las copias.
b) Requisitos de almacenamiento en el propio lugar.
c) Requisitos de almacenamiento en otros lugares.
d) Controles para el acceso autorizado a las copias de respaldo.

Refuerzo R1-Pruebas de recuperación.

– [mp.info.6.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente. Su frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

Refuerzo R2-Protección de las copias de seguridad.

– [mp.info.6.r2.1] Al menos, una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.
– Nivel BAJO: mp.info.6.
– Nivel MEDIO: mp.info.6+ R1.
– Nivel ALTO: mp.info.6+ R1 + R2.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico [mp.s.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.1.1] La información distribuida por medio de correo electrónico se protegerá, tanto en el cuerpo de los mensajes como en los anexos.
– [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.

Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

– [mp.s.1.3] Correo no solicitado, en su expresión inglesa «*spam*».
– [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
– [mp.s.1.5] Código móvil de tipo micro-aplicación, en su expresión inglesa «*applet*».

Se establecerán normas de uso del correo electrónico para el personal. (Ver [org.2]). Estas normas de uso contendrán:

– [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
– [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.1.
– Categoría MEDIA: mp.s.1.
– Categoría ALTA: mp.s.1.

5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	+[R1oR2]	+[R1oR2]	+R2+R3

Requisitos.

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

– [mp.s.2.1] Cuando la información requiera control de acceso se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular, tomando medidas en los siguientes aspectos:

a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator, URL*).
c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.
d) Se prevendrán ataques de inyección de código.

– [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.
– [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

Refuerzo R1-Auditorías de seguridad.

– [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de «caja negra» sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.
– [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

Refuerzo R2-Auditorías de seguridad avanzada.

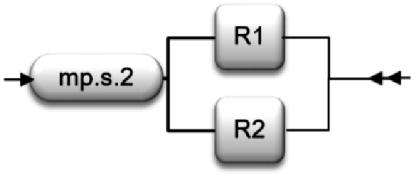
– [mp.s.2.r2.1] Se realizarán auditorías de seguridad de «caja blanca» sobre las aplicaciones web durante la fase de desarrollo.
– [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.
– [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

Refuerzo R3-Protección de las cachés.

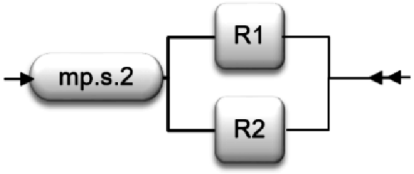
– [mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como "*proxies*" y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como "*cachés*".

Aplicación de la medida.

– Categoría BÁSICA: mp.s.2 + [R1 o R2].



– Categoría MEDIA: mp.s.2 + [R1 o R2].



– Categoría ALTA: mp.s.2 + R2 + R3.

5.8.3 Protección de la navegación web [mp.s.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	+ R1

Requisitos.

El acceso de los usuarios internos a la navegación por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

– [mp.s.3.1] Se establecerá una normativa de utilización, definiendo el uso que se autoriza y las limitaciones de uso personal. En particular, se concretará el uso permitido de conexiones cifradas.
– [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
– [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
– [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
– [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web.
– [mp.s.3.6] Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
– [mp.s.3.7] Se establecerá una política ejecutiva de control de cookies, en particular, para evitar la contaminación entre uso personal y uso organizativo.

Refuerzo R1 - Monitorización.

– [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
– [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Todo

ello sin perjuicio de que se puedan autorizar accesos cifrados singulares a destinos de confianza.

– [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

Refuerzo R2-Destinos autorizados.

– [mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares señalados en la lista blanca estará vetado, salvo autorización singular expresa.

Aplicación de la medida.

– Categoría BÁSICA: mp.s.3.
– Categoría MEDIA: mp.s.3.
– Categoría ALTA: mp.s.3 + R1.

5.8.4 Protección frente a la denegación de servicio [mp.s.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service, DoS y Distributed Denial of Service, DDoS*). Para ello:

– [mp.s 4.1] Se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista.
– [mp.s.4.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

Refuerzo R1-Detección y reacción.

– [mp.s.4.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación de servicio (DoS y DDoS).
– [mp.s. 4.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

Refuerzo R2-Ataques propios.

– [mp.s.4.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

Aplicación de la medida (por disponibilidad).

– Nivel BAJO: no aplica.
– Nivel MEDIO: mp.s.4.
– Nivel ALTO: mp.s.4+ R1.

6. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM)* permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, estás se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) L0-Inexistente.

No existe un proceso que soporte el servicio requerido.

b) L1 - Inicial. Ad hoc.

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostes. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) L2-Reproducible, pero intuitivo.

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) L3-Proceso definido.

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) L4-Gestionado y medible.

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.

f) L5 - Optimizado.

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

Categoría del sistema	Nivel mínimo de madurez requerido
BÁSICA	L2-Reproducible, pero intuitivo.
MEDIA	L3-Proceso definido.
ALTA	L4-Gestionado y medible.

7. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

8. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas de seguridad y en las guías CCN-STIC que sean de aplicación a la implementación y a los diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. Objeto de la auditoría

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos, al objeto de constatar:

a) Que la política de seguridad define los roles y funciones de los responsables del sistema, la información, los servicios y la seguridad del sistema de información.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de «diferenciación de responsabilidades».
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección, tomando como base la Declaración de Aplicabilidad regulada en el artículo 28 de este real decreto.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los siguientes puntos:

a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en artículo 19 «Adquisición de productos de seguridad y contratación de servicios de seguridad».

1.3 Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

2. Niveles de auditoría

Los niveles de auditoría que se realizan a los sistemas de información serán los siguientes:

2.1 Auditoría a sistemas de categoría BÁSICA.

a) Los sistemas de información de categoría BÁSICA no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de la seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento de este real decreto e identificando los hallazgos de conformidad y no conformidad. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.
b) Los informes de auditoría serán analizados por el responsable de la seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

3. Interpretación

La interpretación de este anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información y en la guía CCN-STIC que sea de aplicación, atendiendo al espíritu y finalidad de aquellas.

ANEXO IV

Glosario

– Activo: componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

– Administrador del sistema/de la seguridad del sistema: persona encargada de la instalación y el mantenimiento de un sistema de información, implantando los procedimientos y la configuración de seguridad que se haya establecido en el marco de la política de seguridad del organismo.

– Análisis de riesgos: estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

– Área controlada: zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.

– Arquitectura de seguridad: conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.

– Auditoría de la seguridad: es un proceso sistemático, independiente y documentado que persigue la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

– Autenticación: ratificación de la identidad de un usuario, proceso o dispositivo.

– Autenticación multifactor: exigencia de dos o más factores de autenticación para ratificar una autenticación como válida.

– Autenticador: algo, físico o inmaterial, que posee el usuario bajo su exclusivo control y que le distingue de otros usuarios.

– Autenticidad: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Biometría (factor de autenticación): reconocimiento de los individuos en base a sus características biológicas o de comportamiento.

– Cadena de suministro: conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.

– Categoría de seguridad de un sistema: es un grado, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema de información a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría de seguridad del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

– Certificado de firma electrónica (factor de autenticación): una declaración electrónica que vincula los datos de validación de una firma con una persona física o jurídica y confirma, al menos, el nombre o el seudónimo de esa persona.

– Certificado cualificado de firma electrónica: un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I del Reglamento (UE) 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

– Ciberataque: cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.

– Ciberespacio: dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.

– Ciberincidente: Incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.

– Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Compromiso de la seguridad: incidente de seguridad en el que, debido a una violación de las medidas técnicas u organizativas de seguridad, una información o un servicio quedan expuestos, o potencialmente expuestos, a un acceso no autorizado.

– Confidencialidad: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Contraseña: un secreto memorizado por el usuario, compuesto por varios caracteres según unas reglas de complejidad frente a ataques de adivinación o fuerza bruta.

– Contraseña de un solo uso (*OTP - One-Time Password*): contraseña generada dinámicamente y que solamente se puede usar una vez y durante un periodo limitado.

– Disponibilidad: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Dispositivo de autenticación (*token*): autenticador físico.

– Distintivo de Certificación de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado electrónicamente por la Entidad de Certificación responsable de la evaluación de los sistemas de información concernidos, incluyendo un enlace a la Certificación de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

– Distintivo de Declaración de Conformidad con el ENS: documento electrónico, en formato PDF-A, firmado o sellado electrónicamente por la entidad bajo cuya responsabilidad se encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad con el ENS que, mientras se mantenga su vigencia, permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada de que se trate.

– Dominio de seguridad: colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:

a) Instalaciones centrales, sucursales, comerciales trabajando con portátiles.
b) Servidor central (host), frontal Unix y equipos administrativos.
c) Seguridad física, seguridad lógica.

– Evento de seguridad: ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información, una falla de los controles o una situación desconocida que puede ser relevante para la seguridad.

– Factor de autenticación: hay 3 tipos de factores de autenticación: (1) algo que se sabe, un secreto; (2) algo que se tiene, un autenticador; y (3) algo que se es, biometría.

– Firma electrónica: los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar.

– Firma electrónica avanzada: la firma electrónica que cumple los requisitos contemplados en el artículo 26 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

– Firma electrónica cualificada: una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica.

– Gestión de incidentes: procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante éste.

– Gestión de riesgos: actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.

– Incidente de seguridad (ciberincidente o incidente): suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

– Integridad: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Lista de componentes software: documento que detalla los componentes software utilizados para construir algo, sea una aplicación o un servicio.

– Medidas de seguridad: conjunto de disposiciones encaminadas a proteger al sistema de información de los riesgos a los que estuviere sometido, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

– Mínimo privilegio: principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.

– Monitorización continua: proceso de gestión dinámica de la seguridad basado en el seguimiento de indicadores críticos de seguridad y parcheo de las vulnerabilidades descubiertas en los componentes del sistema de información.

– Observatorio Digital: un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.

– Perfil de cumplimiento específico: conjunto de medidas de seguridad, comprendidas o no en el anexo II de este real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad, y que haya sido habilitado por el CCN.

– PIN: un secreto memorizado por el usuario, compuesto por unos pocos caracteres, siguiendo unas ciertas reglas frente a ataques de adivinación.

– Política de firma electrónica, sello electrónico y certificados: conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas y sellos electrónicos, incluyendo las características exigibles a los certificados de firma o sello electrónicos.

– Política de seguridad (Política de seguridad de la información): conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta.

– Principios básicos de seguridad: fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

– Proceso: conjunto organizado de actividades que se llevan a cabo para producir un producto o prestar un servicio, que tiene un principio y fin delimitados, que implica recursos y da lugar a un resultado.

– Proceso de seguridad: método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

– Proceso TIC: conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio TIC.

– Producto TIC: elemento o grupo de elementos de las redes o los sistemas de información.

– Requisitos mínimos de seguridad: exigencias mínimas necesarias para asegurar la información tratada y los servicios prestados.

– Secreto memorizado (factor de autenticación): algo que solamente sabe el usuario autorizado. Típicamente, se concreta en una contraseña o un PIN.

– Sistema de información: cualquiera de los elementos siguientes:

1.º Las redes de comunicaciones electrónicas que utilice la entidad del ámbito de aplicación de este real decreto sobre las que posea capacidad de gestión.

2.º Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí, en el que uno o varios de ellos realicen, mediante un programa, el tratamiento automático de datos digitales.

3.º Los datos digitales almacenados, tratados, recuperados o transmitidos mediante los elementos contemplados en los números 1.º y 2.º anteriores, incluidos los necesarios para el funcionamiento, utilización, protección y mantenimiento de dichos elementos.

– TEMPEST: término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.

– Trazabilidad: propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) pueden ser trazadas de forma indiscutible hasta dicha entidad.

– USO OFICIAL: designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.

– Usuarios de la organización: personal del organismo, propio o contratado, estable o circunstancial, que acceden al sistema para desarrollar las funciones o actividades que les han sido encomendadas por la organización.

– Usuarios externos: usuarios con acceso al sistema que no entran en el conjunto de usuarios de la organización. En particular, los ciudadanos administrados.

§ 6

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica

Ministerio de la Presidencia
«BOE» núm. 25, de 29 de enero de 2010
Última modificación: 31 de marzo de 2021
Referencia: BOE-A-2010-1331

I

La interoperabilidad es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información.

En el ámbito de las Administraciones públicas, la consagración del derecho de los ciudadanos a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas. Esta obligación tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, así como la remoción de los obstáculos que impidan o dificulten el ejercicio pleno del principio de neutralidad tecnológica y de adaptabilidad al progreso de las tecnologías de la información y las comunicaciones, garantizando con ello la independencia en la elección de las alternativas tecnológicas por los ciudadanos, así como la libertad de desarrollar e implantar los avances tecnológicos en un ámbito de libre mercado.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, reconoce el protagonismo de la interoperabilidad y se refiere a ella como uno de los aspectos en los que es obligado que las previsiones normativas sean comunes y debe ser, por tanto, abordado por la regulación del Estado. La interoperabilidad se recoge dentro del principio de cooperación en el artículo 4 y tiene un protagonismo singular en el título cuarto dedicado a la Cooperación entre Administraciones para el impulso de la administración electrónica. En dicho título el aseguramiento de la interoperabilidad de los sistemas y aplicaciones empleados por las Administraciones públicas figura en el artículo 40 entre las funciones del órgano de cooperación en esta materia, el Comité Sectorial de Administración Electrónica. A continuación, el artículo 41 se refiere a la aplicación por parte de las Administraciones públicas de las medidas informáticas, tecnológicas y organizativas, y de

seguridad, que garanticen un adecuado nivel de interoperabilidad técnica, semántica y organizativa y eviten discriminación a los ciudadanos por razón de su elección tecnológica. Y, seguidamente, el artículo 42.1 crea el Esquema Nacional de Interoperabilidad que comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización que deberán ser tenidos en cuenta por las Administraciones públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad, entre éstas y con los ciudadanos.

La finalidad del Esquema Nacional de Interoperabilidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

II

El Esquema Nacional de Interoperabilidad tiene presentes las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones públicas, así como los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos, así como en su caso y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre acceso electrónico de los ciudadanos a los servicios públicos, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, accesibilidad, uso de lenguas oficiales, reutilización de la información en el sector público y órganos colegiados responsables de la administración electrónica. Se han tenido en cuenta otros instrumentos, tales como el Esquema Nacional de Seguridad, desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio, o antecedentes como los Criterios de Seguridad, Normalización y Conservación de las aplicaciones utilizadas para el ejercicio de potestades.

En términos de las recomendaciones de la Unión Europea se atiende al Marco Europeo de Interoperabilidad, elaborado por el programa comunitario IDABC, así como a otros instrumentos y actuaciones elaborados por este programa y que inciden en alguno de los múltiples aspectos de la interoperabilidad, tales como el Centro Europeo de Interoperabilidad Semántica, el Observatorio y Repositorio de Software de Fuentes Abiertas y la Licencia Pública de la Unión Europea. También se atiende a la Decisión 922/2009 del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009, relativa a las soluciones de interoperabilidad para las administraciones públicas europeas, a los planes de acción sobre administración electrónica en materia de interoperabilidad y de aspectos relacionados, particularmente, con la política comunitaria de compartir, reutilizar y colaborar.

III

Este real decreto se limita a establecer los criterios y recomendaciones, junto con los principios específicos necesarios, que permitan y favorezcan el desarrollo de la interoperabilidad en las Administraciones públicas desde una perspectiva global y no fragmentaria, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, en el ámbito de la Ley 11/2007, de 22 de junio, al objeto de conseguir un común denominador normativo.

En consecuencia, el Esquema Nacional de Interoperabilidad atiende a todos aquellos aspectos que conforman de manera global la interoperabilidad. En primer lugar, se atiende a las dimensiones organizativa, semántica y técnica a las que se refiere el artículo 41 de la Ley 11/2007, de 22 de junio; en segundo lugar, se tratan los estándares, que la Ley 11/2007, de 22 de junio, pone al servicio de la interoperabilidad así como de la independencia en la elección de las alternativas tecnológicas y del derecho de los ciudadanos a elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas; en tercer lugar, se tratan las infraestructuras y los servicios comunes, elementos reconocidos de dinamización, simplificación y propagación de la interoperabilidad, a la vez que facilitadores de la relación multilateral; en cuarto lugar, se trata la reutilización, aplicada a las aplicaciones

de las Administraciones públicas, de la documentación asociada y de otros objetos de información, dado que la voz «compartir» se encuentra presente en la definición de interoperabilidad recogida en la Ley 11/2007, de 22 de junio, y junto con «reutilizar», ambas son relevantes para la interoperabilidad y se encuentran entroncadas con las políticas de la Unión Europea en relación con la idea de compartir, reutilizar y colaborar; en quinto lugar, se trata la interoperabilidad de la firma electrónica y de los certificados; por último, se atiende a la conservación, según lo establecido en la citada Ley 11/2007,de 22 de junio, como manifestación de la interoperabilidad a lo largo del tiempo, y que afecta de forma singular al documento electrónico.

En esta norma se hace referencia a la interoperabilidad como un proceso integral, en el que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

La norma se estructura en doce capítulos, cuatro disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria, tres disposiciones finales y un anexo conteniendo el glosario de términos.

El Esquema Nacional de Interoperabilidad se remite al Esquema Nacional de Seguridad para las cuestiones relativas en materia de seguridad que vayan más allá de los aspectos necesarios para garantizar la interoperabilidad.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42, apartado 3, y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Interoperabilidad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad comprenderá los criterios y recomendaciones de seguridad, normalización y conservación de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones públicas para asegurar un adecuado nivel de interoperabilidad organizativa, semántica y técnica de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias y para evitar la discriminación a los ciudadanos por razón de su elección tecnológica.

Artículo 2. *Definiciones.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el Glosario de Términos incluido en el anexo.

Artículo 3. *Ámbito de aplicación.*

1. El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

2. El Esquema Nacional de Interoperabilidad y sus normas de desarrollo, prevalecerán sobre cualquier otro criterio en materia de política de interoperabilidad en la utilización de medios electrónicos para el acceso de los ciudadanos a los servicios públicos.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Interoperabilidad.*

La aplicación del Esquema Nacional de Interoperabilidad se desarrollará de acuerdo con los principios generales establecidos en el artículo 4 de la Ley 11/2007, de 22 de junio, y con los siguientes principios específicos de la interoperabilidad:

a) La interoperabilidad como cualidad integral.
b) Carácter multidimensional de la interoperabilidad.
c) Enfoque de soluciones multilaterales.

Artículo 5. *La interoperabilidad como cualidad integral.*

La interoperabilidad se tendrá presente de forma integral desde la concepción de los servicios y sistemas y a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

Artículo 6. *Carácter multidimensional de la interoperabilidad.*

La interoperabilidad se entenderá contemplando sus dimensiones organizativa, semántica y técnica. La cadena de interoperabilidad se manifiesta en la práctica en los acuerdos interadministrativos, en el despliegue de los sistemas y servicios, en la determinación y uso de estándares, en las infraestructuras y servicios básicos de las Administraciones públicas y en la publicación y reutilización de las aplicaciones de las Administraciones públicas, de la documentación asociada y de otros objetos de información. Todo ello sin olvidar la dimensión temporal que ha de garantizar el acceso a la información a lo largo del tiempo.

Artículo 7. *Enfoque de soluciones multilaterales.*

Se favorecerá la aproximación multilateral a la interoperabilidad de forma que se puedan obtener las ventajas derivadas del escalado, de la aplicación de las arquitecturas modulares y multiplataforma, de compartir, de reutilizar y de colaborar.

CAPÍTULO III

Interoperabilidad organizativa

Artículo 8. *Servicios de las Administraciones públicas disponibles por medios electrónicos.*

1. Las Administraciones públicas establecerán y publicarán las condiciones de acceso y utilización de los servicios, datos y documentos en formato electrónico que pongan a disposición del resto de Administraciones especificando las finalidades, las modalidades de consumo, consulta o interacción, los requisitos que deben satisfacer los posibles usuarios de los mismos, los perfiles de los participantes implicados en la utilización de los servicios, los protocolos y criterios funcionales o técnicos necesarios para acceder a dichos servicios, los necesarios mecanismos de gobierno de los sistemas interoperables, así como las condiciones de seguridad aplicables. Estas condiciones deberán en todo caso resultar conformes a los principios, derechos y obligaciones contenidos en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de

desarrollo, así como a lo dispuesto en el Esquema Nacional de Seguridad, y los instrumentos jurídicos que deberán suscribir las Administraciones públicas requeridoras de dichos servicios, datos y documentos.

Se potenciará el establecimiento de convenios entre las Administraciones públicas emisoras y receptoras y, en particular, con los nodos de interoperabilidad previstos en el apartado 3 de este artículo, con el objetivo de simplificar la complejidad organizativa sin menoscabo de las garantías jurídicas.

Al objeto de dar cumplimiento de manera eficaz a lo establecido en el artículo 9 de la Ley 11/2007, de 22 de junio, en el Comité Sectorial de Administración electrónica se identificarán, catalogarán y priorizarán los servicios de interoperabilidad que deberán prestar las diferentes Administraciones públicas.

2. Las Administraciones públicas publicarán aquellos servicios que pongan a disposición de las demás administraciones a través de la Red de comunicaciones de las Administraciones públicas españolas, o de cualquier otra red equivalente o conectada a la misma que garantice el acceso seguro al resto de administraciones.

3. Las Administraciones públicas podrán utilizar nodos de interoperabilidad, entendidos como entidades a las cuales se les encomienda la gestión de apartados globales o parciales de la interoperabilidad organizativa, semántica o técnica.

Artículo 9. *Inventarios de información administrativa.*

1. Cada Administración Pública mantendrá actualizado el conjunto de sus inventarios de información administrativa que incluirá, al menos:

a) La relación de los procedimientos administrativos y servicios prestados de forma clasificada y estructurada. Las Administraciones Públicas conectarán electrónicamente sus inventarios con el Sistema de Información Administrativa gestionado por el Ministerio de Política Territorial y Función Pública en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital.

b) La relación de sus órganos administrativos y oficinas orientadas al público y sus relaciones entre ellos. Dicho inventario se conectará electrónicamente con el Directorio Común de Unidades Orgánicas y Oficinas, gestionado por el Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Ministerio de Política Territorial y Función Pública, que proveerá una codificación unívoca.

2. Cada Administración Pública regulará la creación y mantenimiento de estos dos inventarios, en las condiciones que se determinen, con carácter general, por las normas técnicas de interoperabilidad correspondientes; en su caso, las Administraciones Públicas podrán hacer uso de los citados Sistema de Información Administrativa y Directorio Común de Unidades Orgánicas y Oficinas para la creación y mantenimiento de sus propios inventarios. Para la descripción y modelización de los procedimientos administrativos y de los procesos que los soportan será de aplicación lo previsto sobre estándares en el artículo 11.

CAPÍTULO IV

Interoperabilidad semántica

Artículo 10. *Activos semánticos.*

1. Se establecerá y mantendrá actualizada la Relación de modelos de datos de intercambio que tengan el carácter de comunes, que serán de preferente aplicación para los intercambios de información en las Administraciones públicas, de acuerdo con el procedimiento establecido en disposición adicional primera.

2. Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla, titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes, establecerán y publicarán los correspondientes modelos de datos de intercambio que serán de obligatoria aplicación para los intercambios de información en las Administraciones públicas.

3. Los modelos de datos a los que se refieren los apartados 1 y 2, se ajustarán a lo previsto sobre estándares en el artículo 11 y se publicarán, junto con las definiciones y codificaciones asociadas, a través del Centro de Interoperabilidad Semántica de la Administración, según las condiciones de licenciamiento previstas en el artículo 16.

4. Las definiciones y codificaciones empleadas en los modelos de datos a los que se refieren los apartados anteriores tendrán en cuenta lo dispuesto en la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública y el resto de disposiciones que regulan la función estadística.

CAPÍTULO V

Interoperabilidad técnica

Artículo 11. *Estándares aplicables.*

1. Las Administraciones públicas usarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos, al objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología y, de forma que:

a) Los documentos y servicios de administración electrónica que los órganos o Entidades de Derecho Público emisores pongan a disposición de los ciudadanos o de otras Administraciones públicas se encontrarán, como mínimo, disponibles mediante estándares abiertos.

b) Los documentos, servicios electrónicos y aplicaciones puestos por las Administraciones públicas a disposición de los ciudadanos o de otras Administraciones públicas serán, según corresponda, visualizables, accesibles y funcionalmente operables en condiciones que permitan satisfacer el principio de neutralidad tecnológica y eviten la discriminación a los ciudadanos por razón de su elección tecnológica.

2. En las relaciones con los ciudadanos y con otras Administraciones públicas, el uso en exclusiva de un estándar no abierto sin que se ofrezca una alternativa basada en un estándar abierto se limitará a aquellas circunstancias en las que no se disponga de un estándar abierto que satisfaga la funcionalidad satisfecha por el estándar no abierto en cuestión y sólo mientras dicha disponibilidad no se produzca. Las Administraciones públicas promoverán las actividades de normalización con el fin de facilitar la disponibilidad de los estándares abiertos relevantes para sus necesidades.

3. Para la selección de estándares, en general y, para el establecimiento del catálogo de estándares, en particular, se atenderá a los siguientes criterios:

a) El uso de las especificaciones técnicas de las TIC en la contratación pública junto con las definiciones de norma y especificación técnica establecidos en el Reglamento n.º 1025/2012, del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre normalización europea.

b) La definición de estándar abierto establecida en la Ley 11/2007, de 22 de junio, anexo, letra k).

c) Carácter de especificación formalizada.

d) Definición de «coste que no suponga una dificultad de acceso», establecida en el anexo de este real decreto.

e) Consideraciones adicionales referidas a la adecuación del estándar a las necesidades y funcionalidad requeridas; a las condiciones relativas a su desarrollo, uso o implementación, documentación disponible y completa, publicación, y gobernanza del estándar; a las condiciones relativas a la madurez, apoyo y adopción del mismo por parte del mercado, a su potencial de reutilización, a la aplicabilidad multiplataforma y multicanal y a su implementación bajo diversos modelos de desarrollo de aplicaciones.

4. Para el uso de los estándares complementarios a la selección indicada en el apartado anterior, se tendrá en cuenta la definición de «uso generalizado por los ciudadanos» establecida en el anexo del presente real decreto.

5. En cualquier caso los ciudadanos podrán elegir las aplicaciones o sistemas para relacionarse con las Administraciones públicas, o dirigirse a las mismas, siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos. Para facilitar la interoperabilidad con las Administraciones públicas el catálogo de estándares contendrá una relación de estándares abiertos y en su caso complementarios aplicables.

CAPÍTULO VI

Infraestructuras y servicios comunes

Artículo 12. *Uso de infraestructuras y servicios comunes y herramientas genéricas.*

Las Administraciones públicas enlazarán aquellas infraestructuras y servicios que puedan implantar en su ámbito de actuación con las infraestructuras y servicios comunes que proporcione la Administración General del Estado para facilitar la interoperabilidad y la relación multilateral en el intercambio de información y de servicios entre todas las Administraciones públicas.

CAPÍTULO VII

Comunicaciones de las Administraciones públicas

Artículo 13. *Red de comunicaciones de las Administraciones públicas españolas.*

1. Al objeto de satisfacer lo previsto en el artículo 43 de la Ley 11/2007, de 22 de junio, las Administraciones públicas utilizarán preferentemente la Red de comunicaciones de las Administraciones públicas españolas para comunicarse entre sí, para lo cual conectarán a la misma, bien sus respectivas redes, bien sus nodos de interoperabilidad, de forma que se facilite el intercambio de información y de servicios entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados miembros.

La Red SARA prestará la citada Red de comunicaciones de las Administraciones públicas españolas.

2. Para la conexión a la Red de comunicaciones de las Administraciones públicas españolas serán de aplicación los requisitos previstos en la disposición adicional primera.

Artículo 14. *Plan de direccionamiento de la Administración.*

Las Administraciones Públicas aplicarán el Plan de direccionamiento e interconexión de redes en la Administración, desarrollado en la norma técnica de interoperabilidad correspondiente, para su interconexión a través de las redes de comunicaciones.

Artículo 15. *Hora oficial.*

1. Los sistemas o aplicaciones implicados en la provisión de un servicio público por vía electrónica se sincronizarán con la hora oficial, con una precisión y desfase que garanticen la certidumbre de los plazos establecidos en el trámite administrativo que satisfacen.

2. La sincronización de la fecha y la hora se realizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al Centro Español de Metrología y, cuando sea posible, con la hora oficial a nivel europeo.

CAPÍTULO VIII

Reutilización y transferencia de tecnología

Artículo 16. *Condiciones de licenciamiento aplicables.*

1. Las condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos tendrán en cuenta los siguientes aspectos:

a) El fin perseguido es el aprovechamiento y la reutilización de recursos públicos.
b) La completa protección contra su apropiación exclusiva o parcial por parte de terceros.
c) La exención de responsabilidad del cedente por el posible mal uso por parte del cesionario.
d) La no obligación de asistencia técnica o de mantenimiento por parte del cedente.
e) La ausencia total de responsabilidad por parte del cedente con respecto al cesionario en caso de errores o mal funcionamiento de la aplicación.
f) El licenciamiento se realizará por defecto sin contraprestación y sin necesidad de establecer convenio alguno. Sólo se podrá acordar la repercusión parcial del coste de adquisición o desarrollo de las aplicaciones cedidas en aquellos casos en los que este pago repercuta directamente en el incremento de funcionalidades del activo cedido, incluya adaptaciones concretas para su uso en el organismo cesionario, o impliquen el suministro de servicios de asistencia o soporte para su reutilización en el organismo cesionario.

2. Las Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios siempre que la obra derivada mantenga estas cuatro garantías.

3. Para este fin se procurará la aplicación de la Licencia Pública de la Unión Europea, sin perjuicio de otras licencias que garanticen los mismos derechos expuestos en los apartados 1 y 2.
4. A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos:

a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato.
b) Que en el caso de reutilizar activos previamente existentes, la Administración contratante reciba un producto que pueda ofrecer para su reutilización posterior a otras Administraciones Públicas. Además, en el caso de partir de productos de fuentes abiertas, que sea posible declarar como de fuentes abiertas la futura aplicación desarrollada.

Artículo 17. *Directorios de aplicaciones reutilizables.*

1. La Administración General del Estado mantendrá el Directorio general de aplicaciones para su libre reutilización, de acuerdo al artículo 158 de la Ley 40/2015, de 1 octubre, a través del Centro de Transferencia de Tecnología. Este directorio podrá ser utilizado por otras Administraciones Públicas. En el caso de disponer de un directorio propio, deberá garantizar que las aplicaciones disponibles en ese directorio propio se pueden consultar también a través del Centro de Transferencia de Tecnología.
2. Las Administraciones Públicas conectarán los directorios de aplicaciones para su libre reutilización entre sí; y con instrumentos equivalentes del ámbito de la Unión Europea.

3. Las Administraciones Públicas publicarán las aplicaciones reutilizables, en modo producto o en modo servicio, en los directorios de aplicaciones para su libre reutilización, con al menos el siguiente contenido:

a) Código fuente de las aplicaciones finalizadas, en el caso de ser reutilizables en modo producto y haber sido declaradas de fuentes abiertas.
b) Documentación asociada.
c) Condiciones de licenciamiento de todos los activos, en el caso de ser reutilizables en modo producto, o nivel de servicio ofrecido, en el caso de ser reutilizables en modo servicio.
d) Los costes asociados a su reutilización, en el caso de que existieran.

4. Las Administraciones procurarán la incorporación a la aplicación original de aquellas modificaciones o adaptaciones realizadas sobre cualquier aplicación que se haya obtenido desde un directorio de aplicaciones reutilizables.

CAPÍTULO IX

Firma electrónica y certificados

Artículo 18. *Interoperabilidad en la política de firma electrónica y de certificados.*

1. La Administración General del Estado definirá una política de firma electrónica y de certificados que servirá de marco general de interoperabilidad para el reconocimiento mutuo de las firmas electrónicas basadas en certificados de documentos administrativos en las Administraciones Públicas.

Todos los organismos y entidades de derecho público de la Administración General del Estado aplicarán la política de firma electrónica y de certificados a que se refiere el párrafo anterior. La no aplicación de dicha política deberá ser justificada por el órgano u organismo competente y autorizada por la Secretaría General de Administración Digital.

2. Las restantes Administraciones Públicas podrán acogerse a la política de firma electrónica y de certificados a que hace referencia el apartado anterior.

3. Sin perjuicio de lo expuesto en el apartado anterior, las Administraciones Públicas podrán aprobar otras políticas de firma electrónica dentro de sus respectivos ámbitos competenciales.

Las políticas de firma electrónica que aprueben las Administraciones Públicas partirán de la norma técnica establecida a tal efecto en la disposición adicional primera, de los estándares técnicos existentes, y deberán ser interoperables con la política marco de firma electrónica mencionada en el apartado 1, en particular, con sus ficheros de implementación. La Administración Pública proponente de una política de firma electrónica particular garantizará su interoperabilidad con la citada política marco de firma electrónica y con sus correspondientes ficheros de implementación según las condiciones establecidas en la norma técnica de interoperabilidad recogida a tal efecto en la disposición adicional primera.

4. Al objeto de garantizar la interoperabilidad de las firmas electrónicas emitidas conforme a las políticas establecidas, las políticas de firma electrónica que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

5. Las Administraciones Públicas receptoras de documentos electrónicos firmados, siempre que hayan admitido con anterioridad la política de firma del emisor, permitirán la validación de las firmas electrónicas según la política de firma indicada en la firma del documento electrónico.

6. Los perfiles comunes de los campos de los certificados definidos por la política de firma electrónica y de certificados posibilitarán la interoperabilidad entre las aplicaciones usuarias, de manera que tanto la identificación como la firma electrónica generada a partir de estos perfiles comunes puedan ser reconocidos por las aplicaciones de las distintas Administraciones Públicas sin ningún tipo de restricción técnica, semántica u organizativa.

7. Los procedimientos en los que se utilicen certificados de firma electrónica deberán atenerse a la política de firma electrónica y de certificados aplicable en su ámbito, particularmente en la aplicación de los datos obligatorios y opcionales, las reglas de creación

y validación de firma electrónica, los algoritmos a utilizar y longitudes de clave mínimas aplicables.

Artículo 19. *Aspectos de interoperabilidad relativos a los prestadores de servicios de certificación.*

(Suprimido)

Artículo 20. *Plataformas de validación de certificados electrónicos y de firma electrónica.*

1. Las plataformas de validación de certificados electrónicos y de firma electrónica proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones públicas.

2. Proporcionarán, en un único punto de llamada, todos los elementos de confianza y de interoperabilidad organizativa, semántica y técnica necesarios para integrar los distintos certificados reconocidos y firmas que pueden encontrase en los dominios de dos administraciones diferentes.

3. Potenciarán la armonización técnica y la utilización común de formatos, estándares y políticas de firma electrónica y de certificados para las firmas electrónicas entre las aplicaciones usuarias, y de otros elementos de interoperabilidad relacionados con los certificados, tales como el análisis de los campos y extracción univoca de la información pertinente. En particular, se tendrán en cuenta los estándares europeos de las Organizaciones Europeas de Estandarización en el campo de las Tecnologías de Información y Comunicación aplicadas a la firma electrónica.

4. Incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones públicas nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza.

CAPÍTULO X

Recuperación y conservación del documento electrónico

Artículo 21. *Condiciones para la recuperación y conservación de documentos.*

1. Las Administraciones públicas adoptarán las medidas organizativas y técnicas necesarias con el fin de garantizar la interoperabilidad en relación con la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Tales medidas incluirán:

a) La definición de una política de gestión de documentos en cuanto al tratamiento, de acuerdo con las normas y procedimientos específicos que se hayan de utilizar en la formación y gestión de los documentos y expedientes.

b) La inclusión en los expedientes de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del expediente electrónico y permita su recuperación.

c) La identificación única e inequívoca de cada documento por medio de convenciones adecuadas, que permitan clasificarlo, recuperarlo y referirse al mismo con facilidad.

d) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios, asociados al documento electrónico, a lo largo de su ciclo de vida, e incorporación al esquema de metadatos.

e) La clasificación, de acuerdo con un plan de clasificación adaptado a las funciones, tanto generales como específicas, de cada una de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas.

f) El período de conservación de los documentos, establecido por las comisiones calificadoras que correspondan, de acuerdo con la legislación en vigor, las normas administrativas y obligaciones jurídicas que resulten de aplicación en cada caso.

g) El acceso completo e inmediato a los documentos a través de métodos de consulta en línea que permitan la visualización de los documentos con todo el detalle de su contenido, la recuperación exhaustiva y pertinente de los documentos, la copia o descarga en línea en los

formatos originales y la impresión a papel de aquellos documentos que sean necesarios. El sistema permitirá la consulta durante todo el período de conservación al menos de la firma electrónica, incluido, en su caso, el sello de tiempo, y de los metadatos asociados al documento.

h) La adopción de medidas para asegurar la conservación de los documentos electrónicos a lo largo de su ciclo de vida, de acuerdo con lo previsto en el artículo 22, de forma que se pueda asegurar su recuperación de acuerdo con el plazo mínimo de conservación determinado por las normas administrativas y obligaciones jurídicas, se garantice su conservación a largo plazo, se asegure su valor probatorio y su fiabilidad como evidencia electrónica de las actividades y procedimientos, así como la transparencia, la memoria y la identificación de los órganos de las Administraciones públicas y de las Entidades de Derecho Público vinculadas o dependientes de aquéllas que ejercen la competencia sobre el documento o expediente.

i) La coordinación horizontal entre el responsable de gestión de documentos y los restantes servicios interesados en materia de archivos.

j) Transferencia, en su caso, de los expedientes entre los diferentes repositorios electrónicos a efectos de conservación, de acuerdo con lo establecido en la legislación en materia de Archivos, de manera que se pueda asegurar su conservación, y recuperación a medio y largo plazo.

k) Si el resultado del procedimiento de evaluación documental así lo establece, borrado de la información, o en su caso, destrucción física de los soportes, de acuerdo con la legislación que resulte de aplicación, dejando registro de su eliminación.

l) La formación tecnológica del personal responsable de la ejecución y del control de la gestión de documentos, como de su tratamiento y conservación en archivos o repositorios electrónicos.

m) La documentación de los procedimientos que garanticen la interoperabilidad a medio y largo plazo, así como las medidas de identificación, recuperación, control y tratamiento de los documentos electrónicos.

2. A los efectos de lo dispuesto en el apartado 1, las Administraciones públicas crearán repositorios electrónicos, complementarios y equivalentes en cuanto a su función a los archivos convencionales, destinados a cubrir el conjunto del ciclo de vida de los documentos electrónicos.

Artículo 22. *Seguridad.*

1. Para asegurar la conservación de los documentos electrónicos se aplicará lo previsto en el Esquema Nacional de Seguridad en cuanto al cumplimento de los principios básicos y de los requisitos mínimos de seguridad mediante la aplicación de las medidas de seguridad adecuadas a los medios y soportes en los que se almacenen los documentos, de acuerdo con la categorización de los sistemas.

2. Cuando los citados documentos electrónicos contengan datos de carácter personal les será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo.

3. Estas medidas se aplicarán con el fin de garantizar la integridad, autenticidad, confidencialidad, disponibilidad, trazabilidad, calidad, protección, recuperación y conservación física y lógica de los documentos electrónicos, sus soportes y medios, y se realizarán atendiendo a los riesgos a los que puedan estar expuestos y a los plazos durante los cuales deban conservarse los documentos.

4. Los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.

Cuando la firma y los certificados no puedan garantizar la autenticidad y la evidencia de los documentos electrónicos a lo largo del tiempo, éstas les sobrevendrán a través de su conservación y custodia en los repositorios y archivos electrónicos, así como de los metadatos de gestión de documentos y otros metadatos vinculados, de acuerdo con las características que se definirán en la Política de gestión de documentos.

Artículo 23. *Formatos de los documentos.*

1. Con el fin de garantizar la conservación, el documento se conservará en el formato en que haya sido elaborado, enviado o recibido, y preferentemente en un formato correspondiente a un estándar abierto que preserve a lo largo del tiempo la integridad del contenido del documento, de la firma electrónica y de los metadatos que lo acompañan.

2. La elección de formatos de documento electrónico normalizados y perdurables para asegurar la independencia de los datos de sus soportes se realizará de acuerdo con lo previsto en el artículo 11.

3. Cuando exista riesgo de obsolescencia del formato o bien deje de figurar entre los admitidos en el presente Esquema Nacional de Interoperabilidad, se aplicarán procedimientos normalizados de copiado auténtico de los documentos con cambio de formato, de etiquetado con información del formato utilizado y, en su caso, de las migraciones o conversiones de formatos.

Artículo 24. *Digitalización de documentos en soporte papel.*

1. La digitalización de documentos en soporte papel por parte de las Administraciones públicas se realizará de acuerdo con lo indicado en la norma técnica de interoperabilidad correspondiente en relación con los siguientes aspectos:

a) Formatos estándares de uso común para la digitalización de documentos en soporte papel y técnica de compresión empleada, de acuerdo con lo previsto en el artículo 11.

b) Nivel de resolución.

c) Garantía de imagen fiel e íntegra.

d) Metadatos mínimos obligatorios y complementarios, asociados al proceso de digitalización.

2. La gestión y conservación del documento electrónico digitalizado atenderá a la posible existencia del mismo en otro soporte.

CAPÍTULO XI

Normas de conformidad

Artículo 25. *Sedes y registros electrónicos.*

La interoperabilidad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Interoperabilidad.

Artículo 26. *Ciclo de vida de servicios y sistemas.*

La conformidad con el Esquema Nacional de Interoperabilidad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.

Artículo 27. *Mecanismo de control.*

Cada órgano o Entidad de Derecho Público establecerá sus mecanismos de control para garantizar, de forma efectiva, el cumplimiento del Esquema Nacional de Interoperabilidad.

Artículo 28. *Publicación de conformidad.*

Los órganos y Entidades de Derecho Público de las Administraciones públicas darán publicidad, en las correspondientes sedes electrónicas, a las declaraciones de conformidad y a otros posibles distintivos de interoperabilidad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Interoperabilidad.

CAPÍTULO XII

Actualización

Artículo 29. *Actualización permanente.*

El Esquema Nacional de Interoperabilidad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan.

Disposición adicional primera. *Desarrollo del Esquema Nacional de Interoperabilidad.*

1. Se desarrollarán las siguientes normas técnicas de interoperabilidad que serán de obligado cumplimiento por parte de las Administraciones Públicas:

a) Norma Técnica de Catálogo de estándares: establecerá un conjunto de estándares que satisfagan lo previsto en el artículo 11 de forma estructurada y con indicación de los criterios de selección y ciclo de vida aplicados.

b) Norma Técnica de Documento electrónico: tratará los metadatos mínimos obligatorios, la asociación de los datos y metadatos de firma o de sellado de tiempo, así como otros metadatos complementarios asociados; y los formatos de documento.

c) Norma Técnica de Digitalización de documentos: tratará los formatos y estándares aplicables, los niveles de calidad, las condiciones técnicas y los metadatos asociados al proceso de digitalización.

d) Norma Técnica de Expediente electrónico: tratará de su estructura y formato, así como de las especificaciones de los servicios de remisión y puesta a disposición.

e) Norma Técnica de Política de firma electrónica y de certificados de la Administración: Tratará, entre otras cuestiones recogidas en su definición en el anexo, aquellas que afectan a la interoperabilidad incluyendo los formatos de firma, los algoritmos a utilizar y longitudes mínimas de las claves, las reglas de creación y validación de la firma electrónica, la gestión de las políticas de firma, el uso de las referencias temporales y de sello de tiempo, así como la normalización de la representación de la firma electrónica en pantalla y en papel para el ciudadano y en las relaciones entre las Administraciones Públicas.

f) Norma Técnica de Protocolos de intermediación de datos: tratará las especificaciones de los protocolos de intermediación de datos que faciliten la integración y reutilización de servicios en las Administraciones Públicas y que serán de aplicación para los prestadores y consumidores de tales servicios.

g) Norma Técnica de Relación de modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras Administraciones.

h) Norma Técnica de Política de gestión de documentos electrónicos: incluirá directrices para la asignación de responsabilidades, tanto directivas como profesionales, y la definición de los programas, procesos y controles de gestión de documentos y administración de los repositorios electrónicos, y la documentación de los mismos, a desarrollar por las Administraciones Públicas y por los organismos públicos y entidades de derecho público vinculados o dependientes de aquéllas.

i) Norma Técnica de Requisitos de conexión a la Red de comunicaciones de las Administraciones Públicas españolas.

j) Norma Técnica de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, así como desde papel u otros medios físicos a formatos electrónicos.

k) Norma Técnica de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales: tratará de aspectos funcionales y técnicos para el intercambio de asientos registrales, gestión de errores y excepciones, gestión de anexos, requerimientos tecnológicos y transformaciones de formatos.

l) Norma Técnica de Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de información puestos a disposición del público por medios electrónicos para su reutilización.

m) Norma Técnica de interoperabilidad de inventario y codificación de objetos administrativos: tratará las reglas relativas a la codificación de objetos administrativos, así como la conexión entre los inventarios correspondientes, incluyendo, por un lado, las unidades orgánicas y oficinas de la Administración, y, por otro lado, la información administrativa de procedimientos y servicios.

n) Norma Técnica de Interoperabilidad de Transferencia e Ingreso de documentos y expedientes electrónicos: tratará los requisitos y condiciones relativos a la transferencia de agrupaciones documentales en formato electrónico, documentos y expedientes electrónicos, junto con los metadatos asociados, entre sistemas de gestión de documentos electrónicos y sistemas de archivo electrónico.

ñ) Norma Técnica de Interoperabilidad de Valoración y Eliminación de documentos y expedientes electrónicos: tratará las condiciones y requisitos relativos a la valoración de los documentos y expedientes electrónicos para establecimiento de plazos de conservación, transferencia y acceso o, en su caso, eliminación total o parcial.

o) Norma Técnica de Interoperabilidad de preservación de documentación electrónica: tratará las condiciones y requisitos relativos a la conservación de los documentos electrónicos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, así como la protección, recuperación y conservación física y lógica de los documentos y su contexto.

p) Norma Técnica de Interoperabilidad de tratamiento y preservación de bases de datos: tratará las condiciones y requisitos relativos a la conservación de las bases de datos para garantizar su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad, y permitiendo la protección, recuperación y conservación física y lógica de los datos y su contexto.

q) Norma Técnica de Interoperabilidad de Plan de Direccionamiento: tratará reglas aplicables a la asignación y requisitos de direccionamiento IP para garantizar la correcta administración de la Red de comunicaciones de las Administraciones Públicas españolas y evitar el uso de direcciones duplicadas.

r) Norma Técnica de Interoperabilidad de reutilización de activos en modo producto y en modo servicio: tratará los requisitos y condiciones para facilitar la reutilización de activos tanto en modo producto como en modo servicio por las Administraciones Públicas españolas.

s) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros de funcionarios habilitados: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de funcionarios habilitados pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas.

t) Norma Técnica de Interoperabilidad del modelo de datos y condiciones de interoperabilidad de los registros electrónicos de apoderamientos: tratará los aspectos funcionales y técnicos para la plena interoperabilidad de los registros electrónicos de apoderamientos pertenecientes a las Administraciones, así como la interconexión de estos a las sedes electrónicas, A los registros mercantiles, de la propiedad, y a los protocolos notariales.

u) Norma Técnica de Interoperabilidad de Sistema de Referencia de documentos y repositorios de confianza: tratará los requisitos técnicos que deberán cumplir las referencias a documentos al ser intercambiadas, de forma que se evite trasladar documentación de forma innecesaria.

v) Norma Técnica de Política de firma electrónica y de certificados en el ámbito estatal: tratará las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación, organizadas alrededor de los conceptos de generación y validación de firma e incluirá los perfiles interoperables de los medios de identificación de las Administraciones Públicas previstos en Ley 40/2015, de 1 de octubre.

2. El Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica prevista en la disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, aprobará las normas técnicas de interoperabilidad y las publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

3. Para la redacción y actualización de las normas técnicas de interoperabilidad indicadas en el apartado 1 y las futuras que pueda aprobar el Ministerio de Asuntos Económicos y Transformación Digital que sean necesarias para garantizar el adecuado nivel de interoperabilidad como consecuencia del nivel de desarrollo tecnológico, los compromisos internacionales o el marco normativo aplicable, se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de Administración electrónica.

Para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica, el órgano competente será el Centro Criptológico Nacional, adscrito al Centro Nacional de Inteligencia.

4. Se desarrollarán los siguientes instrumentos para la interoperabilidad:

a) Sistema de Información Administrativa: Inventario de procedimientos administrativos, servicios prestados y otras actuaciones administrativas que generen documentación pública, conteniendo información de los mismos clasificada por funciones y con indicación de su nivel de informatización, así como información acerca de las interfaces al objeto de favorecer la interacción o en su caso la integración de los procesos.

b) Centro de interoperabilidad semántica de la Administración: Almacenará, publicará y difundirá los modelos de datos de los servicios de interoperabilidad entre Administraciones Públicas y de estas con los ciudadanos, tanto comunes como sectoriales, así como los relativos a infraestructuras y servicios comunes, además de las especificaciones semánticas y codificaciones relacionadas. Su propósito es facilitar la comprensión semántica de los servicios de intercambio de datos de las Administraciones y maximizar la reutilización de activos semánticos en la construcción de éstos. Se conectará con otros instrumentos equivalentes de las Administraciones Públicas y del ámbito de la Unión Europea.

c) Centro de Transferencia de Tecnología: Directorio de aplicaciones para su libre reutilización que contendrá la relación de aplicaciones para su libre reutilización, incluyendo, al menos, los datos descriptivos relativos a nombre de la aplicación, breve descripción de sus funcionalidades, uso y características, licencia, principales estándares abiertos aplicados, y estado de desarrollo.

d) Directorio Común de Unidades Orgánicas y Oficinas de las Administraciones Públicas: Instrumento que permitirá la sincronización de los sistemas que traten la información de inventariado, codificación y evolución de unidades orgánicas y oficinas en diferentes modalidades de integración para garantizar la flexibilidad tanto en el consumo como en la provisión de información relacionada.

Disposición adicional segunda. *Formación.*

El personal de las Administraciones públicas recibirá la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Interoperabilidad, a cuyo fin los órganos responsables dispondrán lo necesario para que esta formación sea una realidad efectiva.

Disposición adicional tercera. *Centro Nacional de Referencia de Aplicación de las Tecnologías de la Información y la Comunicación (TIC) basadas en fuentes abiertas.*

(Suprimida)

Disposición adicional cuarta. *Instituto Nacional de Tecnologías de la Comunicación.*

(Suprimida)

Disposición adicional quinta. *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.

Disposición transitoria primera. *Adecuación de sistemas y servicios.*

Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán al Esquema Nacional de Interoperabilidad de forma que permitan el cumplimiento de lo establecido en la Disposición final tercera de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.

Si a los doce meses de la entrada en vigor del Esquema Nacional de Interoperabilidad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, se dispondrá de un plan de adecuación, que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

Disposición transitoria segunda. *Uso de medios actualmente admitidos de identificación y autenticación.*

De acuerdo con lo previsto en el artículo 19 de la Ley 11/2007, de 22 de junio, y en la disposición transitoria primera del Real Decreto 1671/2009, de 6 de noviembre, se establece un plazo de adaptación de veinticuatro meses en el que se podrá seguir utilizando los medios actualmente admitidos de identificación y firma electrónica.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones Públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Glosario de términos

Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de informática.

Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

Cadena de interoperabilidad: Expresión de la interoperabilidad en el despliegue de los sistemas y los servicios como una sucesión de elementos enlazados e interconectados, de forma dinámica, a través de interfaces y con proyección a las dimensiones técnica, semántica y organizativa.

Ciclo de vida de un documento electrónico: Conjunto de las etapas o períodos por los que atraviesa la vida del documento, desde su identificación en un sistema de gestión de

documentos, hasta su selección para conservación permanente, de acuerdo con la legislación sobre Archivos de aplicación en cada caso, o para su destrucción reglamentaria.

Coste que no suponga una dificultad de acceso: Precio del estándar que, por estar vinculado al coste de distribución y no a su valor, no impide conseguir su posesión o uso.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Digitalización: El proceso tecnológico que permite convertir un documento en soporte papel o en otro soporte no electrónico en uno o varios ficheros electrónicos que contienen la imagen codificada, fiel e íntegra del documento.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Especificación técnica: Una especificación que figura en un documento en el que se definen las características requeridas de un producto, tales como los niveles de calidad, el uso específico, la seguridad o las dimensiones, incluidas las prescripciones aplicables al producto en lo referente a la denominación de venta, la terminología, los símbolos, los ensayos y métodos de ensayo, el envasado, el marcado y el etiquetado, así como los procedimientos de evaluación de la conformidad.

Especificación formalizada: Aquellas especificaciones que o bien son normas en el sentido de la Directiva 98/34 o bien proceden de consorcios de la industria u otros foros de normalización.

Esquema de metadatos: Instrumento que define la incorporación y gestión de los metadatos de contenido, contexto y estructura de los documentos electrónicos a lo largo de su ciclo de vida.

Estándar: Véase norma.

Estándar abierto: Aquél que reúne las siguientes condiciones:

a) Que sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

b) Que su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

Ficheros de implementación de las políticas de firma: Son la representación en lenguaje formal (XML o ASN.1) de las condiciones establecidas en la política de firma, acorde a las normas técnicas establecidas por los organismos de estandarización.

Firma electrónica: Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Formato: Conjunto de reglas (algoritmo) que define la manera correcta de intercambiar o almacenar datos en memoria.

Herramientas genéricas: Instrumentos y programas de referencia, compartidos, de colaboración o componentes comunes y módulos similares reutilizables que satisfacen las necesidades comunes en los distintos ámbitos administrativos.

Imagen electrónica: Resultado de aplicar un proceso de digitalización a un documento.

Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

Infraestructura o servicio común: capacidad organizativa y técnica que satisface necesidades comunes de los usuarios en diversos ámbitos de la Administración, junto con su gobernanza operativa de apoyo, que pueden tener carácter horizontal o sectorial, con diversos modos de provisión, como servicio o como producto, o integración a modo de plataforma, que facilitan la interoperabilidad, la seguridad, las economías de escala, la racionalización y la simplificación de la actuación administrativa.

Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus

actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

Interoperabilidad semántica: Es aquella dimensión de la interoperabilidad relativa a que la información intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

Interoperabilidad técnica: Es aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

Interoperabilidad en el tiempo: Es aquella dimensión de la interoperabilidad relativa a la interacción entre elementos que corresponden a diversas oleadas tecnológicas; se manifiesta especialmente en la conservación de la información en soporte electrónico.

Licencia Pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las 22 lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

Lista de servicios de confianza (TSL): Lista de acceso público que recoge información precisa y actualizada de aquellos servicios de certificación y firma electrónica que se consideran aptos para su empleo en un marco de interoperabilidad de las Administraciones públicas españolas y europeas.

Marca de tiempo: La asignación por medios electrónicos de la fecha y, en su caso, la hora a un documento electrónico.

Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

Modelo de datos: Conjunto de definiciones (modelo conceptual), interrelaciones (modelo lógico) y reglas y convenciones (modelo físico) que permiten describir los datos para su intercambio.

Nivel de resolución: Resolución espacial de la imagen obtenida como resultado de un proceso de digitalización.

Nodo de interoperabilidad: Organismo que presta servicios de interconexión técnica, organizativa y jurídica entre sistemas de información para un conjunto de Administraciones Públicas bajo las condiciones que éstas fijen.

Norma: Especificación técnica aprobada por un organismo de normalización reconocido para una aplicación repetida o continuada cuyo cumplimiento no sea obligatorio y que esté incluida en una de las categorías siguientes:

a) norma internacional: norma adoptada por una organización internacional de normalización y puesta a disposición del público,

b) norma europea: norma adoptada por un organismo europeo de normalización y puesta a disposición del público,

c) norma nacional: norma adoptada por un organismo nacional de normalización y puesta a disposición del público.

Política de firma electrónica: Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

Política de gestión de documentos electrónicos: Orientaciones o directrices que define una organización para la creación y gestión de documentos auténticos, fiables y disponibles a lo largo del tiempo, de acuerdo con las funciones y actividades que le son propias. La

política se aprueba al más alto nivel dentro de la organización, y asigna responsabilidades en cuanto a la coordinación, aplicación, supervisión y gestión del programa de tratamiento de los documentos a través de su ciclo de vida.

Procedimiento administrativo: Proceso formal regulado jurídicamente para la toma de decisiones por parte de las Administraciones públicas para garantizar la legalidad, eficacia, eficiencia, calidad, derechos e intereses presentes, que termina con una resolución en la que se recoge un acto administrativo; este proceso formal jurídicamente regulado se implementa en la práctica mediante un proceso operativo que coincide en mayor o menor medida con el formal.

Proceso operativo: Conjunto organizado de actividades que se llevan a cabo para producir un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Repositorio electrónico: Archivo centralizado donde se almacenan y administran datos y documentos electrónicos, y sus metadatos.

Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

Servicio de interoperabilidad: Cualquier mecanismo que permita a las Administraciones públicas compartir datos e intercambiar información mediante el uso de las tecnologías de la información.

Soporte: Objeto sobre el cual o en el cual es posible grabar y recuperar datos.

Trámite: Cada uno de los estados y diligencias que hay que recorrer en un negocio hasta su conclusión.

Uso generalizado por los ciudadanos: Usado por casi todas las personas físicas, personas jurídicas y entes sin personalidad que se relacionen o sean susceptibles de relacionarse con las Administraciones públicas españolas.

§ 7

Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos

Ministerio de la Presidencia
«BOE» núm. 234, de 26 de septiembre de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-9741

Durante los últimos años hemos asistido a profundos cambios en la Administración en relación a la utilización de las tecnologías de la información y las comunicaciones (TIC). Cambios caracterizados, en una primera fase, por el uso de estas tecnologías en la automatización y mejora del funcionamiento de los procesos internos de la Administración, en el convencimiento de que el ahorro derivado de la mejora de la eficiencia se trasladaría a los ciudadanos. Posteriormente, por la universalización de Internet y de las tecnologías asociadas que ha propiciado el desarrollo de nuevos servicios y formas de relación con los ciudadanos y empresarios en un camino sin retorno hacia la Administración electrónica.

La confluencia de nuevas tendencias tecnológicas como son los llamados servicios en la nube (cloud computing), la aparición de dispositivos móviles cada vez más inteligentes, la generalización del uso de las redes sociales, la capacidad de análisis de grandes volúmenes de datos (big data) junto con la universalización del uso de Internet, han conformado un nuevo panorama en el que los ciudadanos han adquirido nuevos hábitos y expectativas en la utilización de los servicios digitales en su ocio, en su relación con las empresas y también con las Administraciones Públicas.

La digitalización de los servicios engloba, por una parte, a los servicios electrónicos y a las tecnologías de la información y las comunicaciones, que han sido la base de la Administración electrónica en la que España ha alcanzado un avance reseñable.

Pero la digitalización supone también afrontar nuevos retos y oportunidades. La confluencia de estas nuevas fuerzas tecnológicas lleva a un nuevo panorama en el que la Administración debe ser capaz de adaptarse de manera ágil a nuevas demandas de un entorno cambiante, proporcionar información y servicios digitales en cualquier momento, en cualquier lugar y por diferentes canales, generar nuevas formas de relación con los ciudadanos e innovar nuevos servicios, aprovechando las oportunidades que proporcionan estas tecnologías. Y todo ello debe ser provisto de manera segura, ágil y con eficacia y eficiencia en la utilización de los recursos disponibles.

No se trata por lo tanto de la utilización de las TIC en los procesos de la Administración, sino de crear las dinámicas necesarias para poder adaptar los servicios, procesos, operaciones y las capacidades de la Administración a una realidad que es digital y seguirá evolucionando previsiblemente a gran velocidad.

La Administración debe adoptar una nueva cultura de la información y estar preparada para recoger, generar y tratar grandes volúmenes de información digital sobre sus operaciones, procesos y resultados, que podrá ser puesta convenientemente a disposición de ciudadanos para el impulso de la transparencia, y de empresas y agentes sociales para el fomento de la reutilización de la información del sector público. Asimismo, el desarrollo de las capacidades de análisis transversal de la información permitirá optimizar la gestión, mejorar la toma de decisiones y ofrecer servicios interdepartamentales de manera independiente a la estructura administrativa.

Por otra parte, la universalización de los servicios digitales y las nuevas formas de relación con los ciudadanos permiten conformar una Administración más transparente, en la que los ciudadanos puedan participar en la definición e incluso en el diseño de los servicios públicos, de forma que estos se adapten mejor a las necesidades reales de los ciudadanos en un nuevo modelo de gobernanza.

Todo este entorno supone un nuevo mundo de oportunidades, pero también de amenazas, que deben ser afrontados desde un inicio generando en la Administración las sinergias necesarias para aprovechar el talento de las personas que conforman aquélla, sumando los esfuerzos y recursos disponibles y diseñando una estrategia común para la transformación digital de la Administración, basada en las TIC y orientada a la generación de valor para los ciudadanos.

El informe elaborado por la Comisión para la Reforma de las Administraciones Públicas (CORA), creada por Acuerdo de Consejo de Ministros de 26 de octubre de 2012, y presentado al Consejo de Ministros de 21 de junio de 2013, reconoce este papel fundamental de las TIC y aconseja un tratamiento singular respecto a otros servicios comunes a fin de obtener el máximo de eficacia y de optimización de recursos y aprovechar las oportunidades que supone la actuación coordinada de acuerdo a una estrategia común.

El reconocimiento del papel de las tecnologías de la información y las comunicaciones en la transformación de la Administración estaba ya recogido, entre otras, pero muy especialmente, en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que partía del reconocimiento del insuficiente desarrollo de la administración electrónica, y consideraba que la causa en buena medida se debía a que las previsiones de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común tienen carácter facultativo. Es decir, que dejan en manos de las propias Administraciones determinar si los ciudadanos van a poder de modo efectivo, o no, relacionarse por medios electrónicos con ellas, según que éstas quieran poner en pie los instrumentos necesarios para esa comunicación con la Administración. Por ello esa ley pretendió dar el paso del «podrán» por el «deberán».

La Ley 11/2007, de 22 de junio, consagra la relación con las Administraciones Públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones.

El contexto europeo, la Agenda Digital para Europa, propone también medidas legales para el efectivo desarrollo digital de la Unión Europea. El impulso de una administración digital supone también, por tanto, dar respuesta a los compromisos comunitarios estableciendo así un marco operativo y jurídicamente claro con el fin de eliminar la fragmentación y la ausencia de interoperabilidad, potenciar la ciudadanía digital y prevenir la ciberdelincuencia.

Un buen uso de las TIC, eficiente e integrado, resulta también imprescindible para cumplir con los compromisos que la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno establecen para la Administración.

A esta voluntad de constituir las TIC como herramienta de vertebración de la mejora del funcionamiento de las administraciones responde la creación de la Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado, por Real Decreto 695/2013, de 20 de septiembre. La Dirección se configura, de acuerdo con su norma de creación, como un órgano específico, al más alto nivel, para impulsar y coordinar el necesario proceso de racionalización y transformación de las diversas facetas de la política de tecnologías de la información y de las comunicaciones en todo el ámbito del Sector Público Administrativo Estatal. En virtud del Real Decreto 802/2014, de 19 de septiembre, dicho órgano se adscribe al Ministerio de Hacienda y Administraciones Públicas.

El proceso de transformación que se encomienda a la Dirección de Tecnologías de la Información y las Comunicaciones supone revisar planteamientos organizativos vigentes, algunos de los cuales se ponen de manifiesto en el propio informe CORA, entre ellos, la existencia de un elevado grado de atomización y un alto nivel de independencia en la actuación de los agentes que intervienen en el ámbito de las TIC en la Administración General del Estado y sus Organismos Públicos.

Esta situación propicia una elevada autonomía en la gestión de los fondos y recursos TIC por parte de los diferentes órganos de la Administración Pública, siendo en cada una de ellos donde se toman las decisiones de gastos e inversión, lo que ha dado lugar a una dispersión considerable de recursos y esfuerzos en materia TIC, si bien las Subsecretarías y demás órganos competentes en materia de tecnologías de la información y las comunicaciones, a través de las unidades TIC de la Administración General del Estado y sus Organismos Públicos han sido capaces de atender una demanda creciente de servicios y unas exigencias elevadas, que han situado la oferta actual de servicios en niveles equivalentes o superiores a la media de la Unión Europea.

El modelo de gobernanza sobre el que se asienta este real decreto pretende superar esa situación, con el fin de conseguir una política TIC común a toda la Administración General del Estado y sus Organismos Públicos en un contexto de austeridad en el gasto público basado en la exigencia de eficiencia y corresponsabilidad. La Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, tiene uno de sus pilares en los principios de eficiencia en la asignación y utilización de los recursos públicos. Siguiendo el mandato de esta ley, este real decreto contiene disposiciones en materia de planificación de la acción TIC con implicaciones normativas, organizativas, presupuestarias y contractuales que se encuadran en un marco de planificación plurianual, y de programación y presupuestación, que ha de atender a la situación económica, a los objetivos de política económica y al cumplimiento de los principios de estabilidad presupuestaria y sostenibilidad financiera. En desarrollo de lo que dispone la Ley Orgánica 2/2012, de 27 de abril, este real decreto crea instrumentos para contribuir a una gestión de los recursos públicos orientada a la eficacia, la eficiencia, la economía y la calidad, instrumentos imprescindibles para la aplicación de políticas de racionalización del gasto y de mejora de la gestión del sector público.

La estructura de gobernanza de las TIC en la Administración General del Estado y sus Organismos Públicos ha tenido hasta la fecha sus pilares en los órganos colegiados de Administración electrónica. Por una parte, el Consejo Superior de Administración Electrónica, órgano máximo en materia de Administración electrónica del que han emanado las principales líneas y proyectos de Administración electrónica de la Administración General del Estado. Por otra parte, adscritas a los diferentes departamentos Ministeriales, las Comisiones Ministeriales de Administración electrónica (CMAEs).

Las CMAEs han permitido realizar el seguimiento y control de las diferentes inversiones y gastos TIC en el ámbito Ministerial pero, debido a la propia atomización de las unidades ministeriales, no ha sido posible desarrollar, salvo en algunos Ministerios, la labor de diseñar, junto a las unidades administrativas ministeriales, la estrategia digital que soporte los procesos administrativos sectoriales competencia de cada departamento.

En este sentido, la digitalización de la Administración supone no sólo la transformación de los servicios ofrecidos a medios electrónicos, utilizando para ello las capacidades que ofrecen las TIC, sino que apuesta por el rediseño integral de los procesos y servicios actuales de la Administración, permitiendo nuevos modelos de relación con los ciudadanos y habilitando la prestación de servicios innovadores que no serían realizables sin un necesario cambio cultural.

Es fundamental, por lo tanto, contar con unidades TIC ministeriales, que conozcan profundamente el ámbito de trabajo específico del departamento para diseñar servicios digitales adaptados a las necesidades de ciudadanos y empresas, aprovechando la gran capacitación y el conocimiento especializado del personal TIC para el desarrollo y operación de las aplicaciones sectoriales específicas de cada unidad de negocio. Su principal objetivo será impulsar el proceso de transformación digital de la Administración General del Estado y sus Organismos Públicos, que ha de tener por fin no sólo la automatización de los servicios, sino su rediseño integral, aprovechando las capacidades que permiten las nuevas

tecnologías con el fin de implantar nuevos y mejores modelos de relación con los ciudadanos, con servicios más eficientes que faciliten el crecimiento económico.

En este sentido, las Comisiones Ministeriales actuales deben evolucionar su papel hacia la elaboración del proyecto del plan de acción sectorial del departamento en materia de Administración digital, atendiendo de forma priorizada las propuestas y necesidades de los distintos órganos y organismos públicos afectados y promoviendo la compartición de los servicios. De esta manera, las actuales unidades ministeriales de tecnologías de la información y de las comunicaciones se convertirán en las unidades responsables del soporte y la transformación digital de los diferentes ámbitos departamentales.

Los motivos expuestos anteriormente llevan a la necesidad de rediseñar el modelo de gobernanza de las TIC en la Administración General del Estado y sus Organismos Públicos. El desarrollo de este nuevo modelo se ha encomendado a un órgano de nueva creación, específico y al máximo nivel, la Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado.

Para el diseño de la nueva gobernanza TIC, desde la Dirección de Tecnologías de la Información y las Comunicaciones se han identificado tres objetivos básicos:

Primero, orientar las actuaciones y líneas estratégicas en las TIC de forma que tengan como principal objetivo satisfacer las necesidades derivadas de la estrategia global del Gobierno y disponer de una planificación estratégica común para toda la Administración General del Estado y sus Organismos Públicos.

Segundo, potenciar la Administración digital y las TIC como los instrumentos que permitan hacer sostenible el constante proceso de innovación y mejora en la calidad de los servicios ofrecidos por la administración que demandan ciudadanos y empresas, e incrementar la productividad de los empleados públicos.

Tercero, racionalizar el uso de los recursos informáticos de forma que se consiga una mayor eficiencia, proporcionando un ahorro sustancial de costes de todo tipo, y en especial en el resto de la actividad administrativa, como consecuencia de una mayor homogeneidad y simplicidad mediante el uso de herramientas comunes y servicios compartidos, objetivo de especial interés en un contexto de limitación presupuestaria.

En todo caso, se hace necesario favorecer el diseño de sistemas de compras que sean capaces de conseguir ahorros importantes, adoleciendo el proceso de contratación actual de falta de flexibilidad para aprovechar el estado de madurez del sector TIC español. Esta dispersión de las contrataciones TIC en diferentes unidades ha derivado en una gran diversidad de suministradores en la contratación de productos y servicios idénticos, lo que impacta en mayores costes de mantenimiento y evolución, por lo que es necesario racionalizar el proceso de contratación y dotarlo de mecanismos ágiles que favorezcan el aprovechamiento de economías de escala como consecuencia de la agregación de la demanda. En este sentido, la Dirección de Tecnologías de la Información y las Comunicaciones propondrá a la Dirección General de Racionalización y Centralización de la Contratación los contratos de suministros, obras y servicios en materia TIC que deban ser declarados de contratación centralizada por el titular del Ministerio de Hacienda y Administraciones Públicas.

Asimismo, la Dirección de Tecnologías de la Información y las Comunicaciones, se encargará de alinear las inversiones TIC con los objetivos estratégicos establecidos.

El nuevo modelo de gobernanza TIC persigue centralizar las competencias y los medios para desempeñarlas en un único órgano administrativo en el que se integren todas las unidades TIC de la Administración General del Estado y sus Organismos Públicos, articulándose su interacción con el resto de áreas de la Administración, a las que prestan sus servicios, mediante unos nuevos órganos colegiados que sirvan como canal ágil de información y puesta en común de necesidades y oportunidades de utilización de medios informáticos de forma racional y eficiente.

Ello supondrá, por tanto, la capacitación para la prestación de servicios compartidos TIC a todas las unidades de la Administración General del Estado y sus Organismos Públicos y la definición de una estrategia común que definirá las líneas de actuación en materia TIC de los órganos y organismos de la Administración General del Estado y sus Organismos Públicos.

A tales efectos, se crean la Comisión de Estrategia TIC y, en el ámbito departamental, las Comisiones Ministeriales de Administración Digital como órganos colegiados encargados de impulsar la transformación digital de la Administración de acuerdo a una Estrategia común en el ámbito de las Tecnologías de la Información y las Comunicaciones. Asimismo, este real decreto deroga el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica, quedando suprimidos el Consejo Superior de Administración Electrónica y las Comisiones Ministeriales de Administración Electrónica. Este nuevo modelo de Gobernanza en el ámbito de las Tecnologías de la Información y las Comunicaciones se alcanzará de manera paulatina en un proceso que, partiendo desde la heterogeneidad y dispersión actual converja hacia un modelo de prestación de servicios compartidos e infraestructuras comunes de forma que pueda garantizarse el mantenimiento del nivel de servicio actual y la paulatina implementación de sinergias e incremento de eficiencia, simplificación de estructuras y, por tanto, mejora de la productividad de la Administración.

Para hacer efectivas estas medidas, este real decreto no sólo se aplica a la Administración General del Estado, sus organismos autónomos y entidades gestoras y servicios comunes de la Seguridad Social, sino que se prevé su aplicación a otras entidades públicas, cuya actuación pueda presentar una especial trascendencia en la prestación de servicios públicos electrónicos y en el propio desarrollo de la Administración digital.

En su virtud, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, y del Ministro de Hacienda y Administraciones Públicas, y previa deliberación del Consejo de Ministros en su reunión del día 19 de septiembre de 2014,

DISPONGO:

CAPÍTULO I

Objeto y ámbito de aplicación

Artículo 1. *Objeto.*

El objeto de este real decreto es el desarrollo y ejecución de un modelo común de gobernanza de las Tecnologías de la Información y las Comunicaciones (TIC) en la Administración General del Estado y sus Organismos Públicos.

Este modelo de Gobernanza de las TIC incluirá, en todo caso, la definición e implementación de una estrategia global de transformación digital que garantice el uso adecuado de los recursos informáticos de acuerdo a las necesidades derivadas de la estrategia general del Gobierno, con el fin de mejorar la prestación de los servicios públicos al ciudadano.

Artículo 2. *Ámbito de aplicación.*

El ámbito de aplicación de este real decreto se extiende a la Administración General del Estado y sus Organismos Públicos previstos en el artículo 43 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

CAPÍTULO II

Órganos con competencias en materia de Administración digital

Artículo 3. *La Comisión de Estrategia TIC. Objeto, adscripción y funcionamiento.*

1. La Comisión de Estrategia TIC es el órgano colegiado encargado de la definición y supervisión de la aplicación de la Estrategia sobre Tecnologías de la Información y las Comunicaciones de la Administración General del Estado y sus organismos públicos, «Estrategia TIC», que será aprobada por el Gobierno de acuerdo con lo previsto en el artículo 9 de este Real Decreto.

2. La Comisión de Estrategia TIC se adscribe al Ministerio de Hacienda y Administraciones Públicas a través de la Secretaría de Estado de Administraciones Públicas.

3. La Comisión de Estrategia TIC actuará en pleno y por medio de su comité ejecutivo.

Artículo 4. *Funciones de la Comisión de Estrategia TIC.*

1. Corresponde a la Comisión de Estrategia TIC el ejercicio de las siguientes funciones:

a) Fijar las líneas estratégicas, de acuerdo con la política establecida por el Gobierno, en materia de tecnologías de la información y las comunicaciones, para el impulso de la Administración digital en la Administración General del Estado y sus organismos públicos.

b) Aprobar la propuesta de Estrategia TIC de la Administración General del Estado y sus organismos públicos para su elevación al Consejo de Ministros por los titulares de los departamentos de Hacienda y Administraciones Públicas y de la Presidencia.

c) Informar los anteproyectos de ley, los proyectos de disposiciones reglamentarias y otras normas de ámbito general que le sean sometidos por los órganos proponentes cuyo objeto sea la regulación en materia TIC de aplicación en la Administración General del Estado y sus Organismos Públicos o de los recursos de carácter material y humano afectos a su desarrollo.

d) Definir las prioridades de inversión en materias TIC de acuerdo con los objetivos establecidos por el Gobierno.

e) Declarar los medios o servicios compartidos en los términos establecidos en el artículo 10.

f) Declarar los proyectos de interés prioritario, en los términos establecidos en el artículo 11, a propuesta de los ministerios y sus organismos públicos adscritos previo informe de la Dirección de Tecnologías de la Información y las Comunicaciones. Se considerarán proyectos de interés prioritario aquellos que por sus especiales características sean fundamentales para la mejora de la prestación de servicios al ciudadano.

g) Impulsar la colaboración y cooperación con las comunidades autónomas y las entidades locales para la puesta en marcha de servicios interadministrativos integrados y la compartición de infraestructuras técnicas y los servicios comunes que permitan la racionalización de los recursos TIC a todos los niveles del Estado.

h) Impulsar las actividades de cooperación de la Administración General del Estado y sus Organismos Públicos con la Unión Europea, con las organizaciones internacionales y, especialmente, con Iberoamérica, en materia de tecnologías de la información y Administración digital, en colaboración con el Ministerio de Asuntos Exteriores y de Cooperación.

i) Actuar como Observatorio de la Administración Electrónica y Transformación Digital.

2. La Comisión de Estrategia TIC elevará anualmente, a través de su Presidente, un informe al Consejo de Ministros, en el que se recogerá el estado de la transformación digital de la Administración en la Administración General del Estado y sus organismos públicos.

Artículo 5. *Composición y funcionamiento del Pleno de la Comisión de Estrategia TIC.*

1. El Pleno de la Comisión de Estrategia TIC estará integrado por los titulares de las Secretarías de Estado de Administraciones Públicas, de Telecomunicaciones y para la Sociedad de la Información y de Seguridad Social, así como por los Subsecretarios o, bien, el titular de un órgano superior de los distintos Departamentos ministeriales y el Director de Tecnologías de la Información y las Comunicaciones. Será presidido por el Ministro de Hacienda y Administraciones Públicas y actuará como Secretario el Director de Tecnologías de la Información y las Comunicaciones.

2. Las reuniones del Pleno se celebrarán, al menos, dos veces al año por convocatoria de su Presidente, bien a iniciativa propia, bien cuando lo soliciten, al menos, la mitad de sus miembros.

3. El Presidente podrá invitar a incorporarse, con voz pero sin voto, a representantes de otras instituciones públicas o privadas.

4. Las funciones de asistencia y apoyo a la Comisión de Estrategia TIC y a su Comité Ejecutivo serán desempeñadas por la Dirección de Tecnologías de la Información y las Comunicaciones.

5. Por acuerdo de la Comisión de Estrategia TIC se podrán constituir los grupos de trabajo que se requieran para el adecuado desarrollo de sus funciones.

Artículo 6. *Composición y funcionamiento del Comité Ejecutivo de la Comisión de Estrategia TIC.*

1. El Comité Ejecutivo de la Comisión de Estrategia TIC se constituye como el instrumento de la Comisión de Estrategia TIC para asegurar una actuación ágil y efectiva de la Estrategia TIC en la Administración General del Estado y sus Organismos Públicos.

2. El Comité Ejecutivo de la Comisión de Estrategia TIC estará presidido por el Director de Tecnologías de la Información y las Comunicaciones, estará compuesto por un mínimo de cinco miembros, un máximo de diez miembros y su composición será determinada por la Comisión de Estrategia TIC.

Actuará como secretario un funcionario de la Dirección de Tecnologías de la Información y las Comunicaciones, que será designado por el Presidente del Comité.

3. El Comité Ejecutivo ejercerá las competencias que le atribuya expresamente el Pleno de la Comisión de Estrategia TIC, y deberá informar periódicamente a éste acerca de las decisiones y actuaciones adoptadas. En todo caso, le corresponde la aprobación de los Planes de Acción Departamentales regulados en el artículo 14 del presente real decreto.

4. Las reuniones del Comité Ejecutivo se celebrarán mensualmente. El Presidente podrá convocar al Comité con carácter extraordinario cuando resulte necesario.

5. El Presidente del Comité Ejecutivo podrá invitar a incorporarse, con voz pero sin voto, a los Presidentes de las Comisiones Ministeriales de Administración Digital cuando lo estime conveniente.

6. Podrán constituirse los grupos de trabajo que se requieran para el adecuado desarrollo de sus funciones.

Artículo 7. *Las Comisiones Ministeriales de Administración Digital.*

1. Las Comisiones Ministeriales de Administración Digital (CMAD) son órganos colegiados de ámbito departamental responsables del impulso y de la coordinación interna en cada departamento en materia de Administración digital, y serán los órganos de enlace con la Dirección de Tecnologías de la Información y las Comunicaciones.

Las CMAD estudiarán y planificarán las necesidades funcionales de las distintas áreas administrativas del ministerio, valorarán las posibles vías de actuación, priorizándolas, y propondrán su desarrollo, todo ello evitando que se generen duplicidades, conforme al principio de racionalización, y promoviendo la compartición de infraestructuras y servicios comunes.

El ámbito de actuación de las CMAD comprende todos los órganos del departamento y a los organismos públicos adscritos al mismo.

2. Las CMAD estarán presididas por el Subsecretario y estarán integradas por los representantes, con rango mínimo de Subdirector General, de las áreas funcionales y de los organismos adscritos que se determine mediante orden ministerial, así como los responsables de las unidades ministeriales de tecnologías de la información y las comunicaciones.

El Presidente de la CMAD podrá delegar esta función en el titular de una unidad del mismo departamento, con rango mínimo de Director General.

Podrán asistir a las reuniones de la CMAD expertos de la Dirección de Tecnologías de la Información y las Comunicaciones, que tendrán carácter de asesores, con voz y sin voto.

3. Las CMAD desempeñarán las siguientes funciones:

a) Actuar como órgano de relación entre los departamentos ministeriales y sus organismos adscritos y la Dirección de Tecnologías de la Información y las Comunicaciones, para asegurar la coordinación con los criterios y políticas definidas por ésta.

b) Impulsar, ejecutar y supervisar, en el ámbito del departamento, el cumplimiento de las directrices y el seguimiento de las pautas de actuación recogidas en la Estrategia TIC de la Administración General del Estado y sus Organismos Públicos aprobada por el Gobierno a propuesta del Comité de Estrategia TIC.

c) Elaborar el Plan de acción del departamento para la transformación digital, en desarrollo de los criterios establecidos por la Dirección de Tecnologías de la Información y las Comunicaciones atendiendo a la Estrategia TIC de la Administración General del Estado y sus Organismos Públicos, aprobada por el Consejo de Ministros.

d) Analizar las necesidades funcionales de las unidades de gestión del departamento y sus organismos adscritos y evaluar las distintas alternativas de solución propuestas por las unidades TIC, identificando las oportunidades de mejora de eficiencia que pueden aportar las TIC, aplicando soluciones ya desarrolladas en el ámbito del Sector Público y estimando costes en recursos humanos y materiales que los desarrollos TIC asociados puedan suponer

e) Impulsar la digitalización de los servicios y procedimientos del departamento con el fin de homogeneizarlos, simplificarlos, mejorar su calidad y facilidad de uso, así como las prestaciones ofrecidas a los ciudadanos y empresas, optimizando la utilización de los recursos TIC disponibles.

f) Colaborar con la Dirección de Tecnologías de la Información y las Comunicaciones en la identificación y la puesta a disposición común de los medios humanos, materiales y económicos que estén adscritos al departamento y que deban ser utilizados para la puesta en funcionamiento o mantenimiento de los medios o servicios compartidos.

g) Cualesquiera otras que determinen sus respectivas órdenes ministeriales reguladoras, de acuerdo con las peculiares necesidades de cada departamento ministerial.

4. Las CMAD analizarán los proyectos de disposiciones de carácter general de su departamento y elaborarán un informe en el que se expondrán y valorarán la oportunidad de la medida, los costes, necesidad de disponibilidad de recursos humanos y tiempos de desarrollo que se puedan derivar de la aprobación del proyecto desde la perspectiva de la utilización de medios y servicios TIC y lo remitirán a la Dirección de Tecnologías de la Información y las Comunicaciones para su conocimiento y valoración.

5. En el ejercicio de sus funciones y en su ámbito de actuación ministerial, las CMAD, formularán propuestas de aplicación de nuevos criterios de organización o de funcionamiento, implantación de nuevos procedimientos o de revisión de los existentes.

Artículo 8. *El Comité de Dirección de las Tecnologías de Información y Comunicaciones.*

El Comité de Dirección de las Tecnologías de Información y las Comunicaciones es un órgano de apoyo adscrito a la Dirección de Tecnologías de la Información y las Comunicaciones.

Estará integrado por el responsable TIC de las subsecretarías del órgano superior al que corresponda la coordinación de las TIC en cada uno de los departamentos ministeriales así como por los responsables de aquellas unidades TIC que por su relevancia sean designados por el Director de Tecnologías de la Información y las Comunicaciones, quién lo presidirá.

Actuará como órgano de coordinación y colaboración entre la Dirección de Tecnologías de la Información y las Comunicaciones y los órganos y organismos integrantes de la Administración General del Estado y sus Organismos Públicos a fin de establecer una acción coordinada, de acuerdo con las líneas estratégicas definidas por la Comisión de Estrategia TIC y contribuirá a definir metodologías, procesos, arquitecturas, normas y buenas prácticas comunes a todas las unidades TIC de la Administración General del Estado y sus Organismos Públicos velando por el cumplimiento de programas y proyectos, la consecución de los objetivos marcados y la eliminación de redundancias.

CAPÍTULO III

Modelo de gobernanza en el ámbito de las tecnologías de la información y las comunicaciones

Artículo 9. *Estrategia en materia de tecnologías de la información y las comunicaciones.*

El Gobierno, a iniciativa de la Comisión de Estrategia TIC, y a propuesta de los Ministros de la Presidencia, de Hacienda y Administraciones Públicas y de Industria, Energía y Turismo, aprobará la Estrategia en materia de tecnologías de la información y las comunicaciones (en adelante Estrategia TIC), así como las revisiones de la misma.

La Estrategia TIC determinará los objetivos, principios y acciones para el desarrollo de la administración digital y la transformación digital de la Administración General del Estado y sus Organismos Públicos y servirá de base para la elaboración por los distintos ministerios de sus planes de acción para la transformación digital.

La Comisión de Estrategia TIC determinará el ámbito temporal de la Estrategia TIC, así como su periodo de revisión.

Artículo 10. *Medios y servicios compartidos.*

1. Los medios y servicios TIC de la Administración General del Estado y sus Organismos Públicos serán declarados de uso compartido cuando, en razón de su naturaleza o del interés común, respondan a necesidades transversales de un número significativo de unidades administrativas.

A los efectos de este real decreto, se entenderá por «medios y servicios» todas las actividades, infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información.

Los activos TIC afectos a la prestación de servicios sectoriales se podrán mantener en sus ámbitos específicos en razón de la singularidad competencial y funcional que atienden y no tendrán, por tanto, la consideración de medios y servicios compartidos. La responsabilidad sobre la gestión de estos medios corresponderá a los departamentos ministeriales y organismos adscritos desarrollada a través de las respectivas unidades TIC con el apoyo y supervisión de la Dirección de Tecnologías de la Información y las Comunicaciones.

2. La declaración de medios y servicios compartidos necesarios para la ejecución y desarrollo de la Estrategia TIC aprobada por el Gobierno, corresponderá a la Comisión de Estrategia TIC a propuesta de la Dirección de Tecnologías de la Información y las Comunicaciones.

Cuando concurran razones económicas, técnicas o de oportunidad sobrevenidas, la Comisión de Estrategia TIC podrá autorizar al Director de Tecnologías de la Información y las Comunicaciones a acordar excepciones a la declaración de medio o servicio de uso compartido, de las que se dará traslado a los miembros de la Comisión de Estrategia TIC.

La declaración de medio o servicio compartido habilitará a la Dirección de Tecnologías de la Información y las Comunicaciones para adoptar las medidas necesarias para su provisión compartida, bien directamente o a través de otras unidades TIC y, en su caso, para disponer tanto de los medios humanos y económicos como de las infraestructuras y resto de activos TIC que los ministerios y unidades dependientes venían dedicando a atender dichos servicios, entre los que se incluyen también ficheros electrónicos y licencias.

Dada la naturaleza funcional específica y régimen competencial singular de los servicios de Informática presupuestaria de la Intervención General de la Administración del Estado, lo establecido en este apartado 2 respecto a los servicios, recursos e infraestructuras TIC comunes y al catálogo de servicios TIC comunes, cuando pueda afectar a los sistemas de funcionalidad específica de Informática presupuestaria requerirá la previa aprobación de la Intervención General de la Administración del Estado.

3. La utilización de los medios y servicios compartidos será de carácter obligatorio y sustitutivo respecto a los medios y servicios particulares empleados por las distintas unidades.

La Dirección de Tecnologías de la Información y las Comunicaciones establecerá un Catálogo de Servicios Comunes del que formarán parte los medios y servicios compartidos, así como aquellas infraestructuras técnicas o aplicaciones desarrolladas por la Dirección de Tecnologías de la Información y las Comunicaciones cuya provisión de manera compartida facilite la aplicación de economías de escala y contribuya a la racionalización y simplificación de la actuación administrativa.

4. Dentro de este Catálogo figurarán servicios de administración digital orientados a integrar todas las relaciones de las Administraciones públicas con el ciudadano, mediante la provisión compartida, que le permita tener una visión integral de sus relaciones con las Administraciones públicas y acceso a todos los servicios on-line.

5. La provisión, explotación y gestión de los medios y servicios compartidos será realizada por la Dirección de Tecnologías de la Información y las Comunicaciones, salvo los que correspondan a los servicios de informática presupuestaria de la Intervención General de la Administración del Estado. Las eficiencias que se produzcan en estos procesos se dedicarán preferentemente a potenciar los servicios sectoriales.

6. Las CMAD y las unidades TIC sectoriales velarán por el uso de los medios y servicios compartidos. En este sentido, cuando las necesidades puedan ser comunes a más de un área funcional o unidad, del mismo o de distinto ministerio, se escogerá la alternativa que permita compartir el servicio entre dichas áreas, salvo autorización expresa de la Dirección de Tecnologías de la Información y las Comunicaciones.

7. La Dirección de Tecnologías de la Información y las Comunicaciones llevará un registro de los costes que son imputables a cada uno de los diferentes órganos y organismos usuarios, sin perjuicio de las competencias de otros órganos administrativos en materia de control de gasto.

8. La puesta a disposición común de los medios y servicios compartidos se hará de acuerdo con lo previsto en la normativa que resulte aplicable en cada ámbito en materia de personal, organización, presupuestos y patrimonial.

Artículo 11. *Proyectos de interés prioritario.*

El Comité de Estrategia TIC podrá declarar como proyectos de interés prioritario aquellos que tengan una singular relevancia y, especialmente, aquellos que tengan como objetivo la colaboración y cooperación con las comunidades autónomas y los entes que integran la Administración local y la Unión Europea en materia de Administración digital.

La declaración de proyecto de interés prioritario se trasladará como recomendación al Ministerio de Hacienda y Administraciones Públicas y a la Comisión de Políticas de Gasto para que, en su caso, sea tenida en cuenta en la elaboración de los Presupuestos Generales del Estado.

Artículo 12. *Unidades TIC.*

1. Son unidades TIC aquellas unidades administrativas cuya función sea la provisión de servicios en materia de Tecnologías de la Información y Comunicaciones a sí mismas o a otras unidades administrativas.

Las unidades TIC, bajo la dirección de los órganos superiores o directivos a los que se encuentren adscritas, se configuran como instrumentos fundamentales para la implementación y desarrollo de la Estrategia TIC y del proceso de transformación digital de los ámbitos sectoriales de la Administración General del Estado y sus Organismos Públicos bajo la coordinación y supervisión de la Dirección de Tecnologías de la Información y las Comunicaciones.

2. Se entenderá por provisión de servicios TIC la realización de una o varias de las siguientes funciones:

a) Soporte, operación, implementación y/o gestión de sistemas informáticos corporativos o de redes de telecomunicaciones.

b) Desarrollo de aplicativos informáticos en entornos multiusuario.

c) Consultoría informática.

d) Seguridad de sistemas de información.

e) Atención técnica a usuarios.

f) Innovación en el ámbito de las TIC

g) Administración digital.

h) Conformar la voluntad de adquisición de bienes o servicios en el ámbito de las tecnologías de la información y las comunicaciones

i) Todas aquellas funciones no previstas expresamente en las letras anteriores, que sean relevantes en materia de tecnologías de la información y las comunicaciones.

3. Las unidades TIC adscritas a los departamentos ministeriales o a sus organismos adscritos, impulsarán, en el marco de la CMAD, la transformación digital de los servicios sectoriales en sus ámbitos. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá a los órganos competentes, las áreas administrativas que deban ser atendidas por las unidades TIC de manera que se adapten a las nuevas necesidades derivadas de la declaración de medios o servicios compartidos con el fin de mejorar la eficiencia y operatividad en la prestación de sus servicios. Las unidades TIC deberán llevar a cabo dicha transformación identificando las oportunidades que les permitan sacar el máximo

rendimiento a las TIC de acuerdo a las necesidades funcionales determinadas por las áreas administrativas a las que prestan sus servicios.

Artículo 13. *Cooperación interadministrativa.*

1. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá a la Secretaría de Estado de Administraciones Públicas las líneas de actuación, orientaciones comunes y la creación de órganos de cooperación necesarios para favorecer el intercambio de ideas, estándares, tecnología y proyectos orientados a garantizar la interoperabilidad y mejorar la eficacia y eficiencia en la prestación de los servicios públicos de las distintas Administraciones Públicas, que serán tratadas en la Conferencia Sectorial de Administraciones Públicas, en cuyo seno se establecerán.

2. La Dirección de Tecnologías de la Información y las Comunicaciones propondrá al Secretario de Estado de Administraciones Públicas la designación de los representantes de la Administración General del Estado y sus Organismos Públicos en las comisiones o grupos que la Conferencia Sectorial de Administraciones Públicas cree en materia de tecnologías de la información y Administración digital.

CAPÍTULO IV

Actuaciones en relación con la planificación en materia de Administración digital

Artículo 14. *Planes de acción departamentales para la transformación digital.*

1. Cada ministerio contará con un Plan de acción para la transformación digital, que comprenderá las actuaciones en materia de Administración digital, tecnologías de la información y comunicaciones a desarrollar en el conjunto del departamento y sus organismos públicos adscritos.

2. La propuesta del plan se elaborará de acuerdo con las directrices de la Dirección de Tecnologías de la Información y las Comunicaciones y las líneas estratégicas establecidas por el Comité de Estrategia TIC y recogerá de forma concreta los servicios que el ministerio tiene previsto desarrollar, especialmente los dirigidos a la prestación de servicios a ciudadanos y empresas, su planificación temporal, los recursos humanos, técnicos y financieros necesarios y los contratos que se deben realizar.

La propuesta de plan de acción departamental se remitirá por el presidente de la CMAD a la Dirección de Tecnologías de la Información y las Comunicaciones para su estudio y valoración y posterior elevación a la Comisión de Estrategia de Tecnologías de la Información y las Comunicaciones, a efectos del informe preceptivo del Comité Ejecutivo, previo a su aprobación por el órgano competente en el departamento ministerial.

En el plan de acción remitido podrán excluirse los medios y servicios específicos que afecten a la defensa, consulta política, situaciones de crisis y seguridad del Estado y los que manejen información clasificada, de acuerdo con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales.

3. Los planes de acción para la trasformación digital tendrán un alcance, al menos, de dos años.

Artículo 15. *Modificación de los Planes de acción departamentales para la transformación digital.*

La modificación de los Planes de acción departamentales para la transformación digital deberá ser informada por la Dirección de Tecnologías de la Información y las Comunicaciones.

CAPÍTULO V

Actuaciones en relación con la contratación en materia de tecnologías de la información

Artículo 16. *Competencias para el informe técnico de la memoria y los pliegos de prescripciones técnicas para la contratación de tecnologías de la información.*

1. La Dirección de Tecnologías de la Información y las Comunicaciones elaborará y trasladará a los órganos competentes en materia de contratación, los criterios y directrices para la agregación y planificación de la demanda TIC en la Administración General del Estado y sus Organismos Públicos para una mayor eficiencia económica y su configuración como cliente único frente a proveedores externos.

2. La Dirección de Tecnologías de la Información y las Comunicaciones informará con carácter preceptivo la declaración de contratación centralizada, que corresponde al Ministro de Hacienda y Administraciones Públicas a propuesta de la Dirección General de Racionalización y Centralización de la Contratación, de los contratos de suministros, obras y servicios en materia TIC.

Asimismo, para la contratación centralizada en materia TIC la Dirección de Tecnologías de la Información y las Comunicaciones establecerá los criterios técnicos y de oportunidad y la Dirección General de Racionalización y Centralización de la Contratación establecerá los criterios de contratación administrativa y gestión económica.

La Dirección de Tecnologías de la Información y las Comunicaciones realizará el informe técnico preceptivo de la memoria y los pliegos de prescripciones técnicas de las siguientes contrataciones de bienes y servicios informáticos:

a) El suministro de equipos y programas para el tratamiento de la información, de acuerdo con lo establecido en el artículo 9.3 b) del texto refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre.

b) Los contratos de servicios, de acuerdo con lo establecido en el artículo 10 del texto refundido de la Ley de Contratos del Sector Público.

c) Los procedimientos especiales de adopción de tipo realizados al amparo del artículo 206 del texto refundido Ley de Contratos del Sector Público.

d) Los convenios de colaboración y encomiendas de gestión que incluyan la prestación de servicios en materia de tecnologías de la información, comunicaciones o Administración Digital en el ámbito de la Administración General del Estado y sus Organismos Públicos.

3. Estarán excluidos del informe técnico a que se refiere el apartado anterior los contratos comprendidos en el ámbito de aplicación de la Ley 24/2011, de 1 de agosto, de Contratos del sector público en los ámbitos de la defensa y de la seguridad, así como los tramitados de conformidad con el artículo 170.f) del texto refundido de la Ley de Contratos del Sector Público.

La Dirección de Tecnologías de la Información y las Comunicaciones recibirá la información necesaria sobre estas contrataciones a efectos estadísticos, de inventario y presupuestarios necesarios para el gobierno integral de las TIC. En cualquier caso, la recepción de la información se manejará y custodiará de acuerdo a la clasificación establecida y, en su caso, con lo dispuesto en la legislación reguladora de los secretos oficiales y en los Acuerdos internacionales.

Artículo 17. *Tramitación telemática de los informes a la memoria y los pliegos de prescripciones técnicas.*

1. La tramitación de los informes técnicos se regulará mediante instrucción de la Dirección de Tecnologías de la Información y las Comunicaciones y se hará procurando el empleo de medios telemáticos en todas las fases del procedimiento.

2. La tramitación de los informes técnicos se realizará bajo los principios de simplicidad, celeridad y eficacia, y se racionalizarán los trámites administrativos para lograr su máxima sencillez y funcionalidad.

3. El informe técnico se emitirá en el plazo máximo de diez días hábiles posteriores al día en que la unidad TIC registró la documentación completa del expediente de contratación.

Si por causas justificadas el informe previsto en el apartado anterior no pudiera ser emitido en el plazo previsto, se comunicará telemáticamente al órgano solicitante indicando si puede proseguir el procedimiento de contratación o si el informe se considera determinante para la prosecución del procedimiento de contratación, de suscripción de convenio o atribución de encomienda de gestión. En el caso de que el informe se considere determinante se indicará en la comunicación el nuevo plazo en que será evacuado, que no podrá superar 5 días hábiles, transcurrido el cuál sin la emisión del informe podrá proseguir la tramitación del expediente.

4. Las Unidades TIC proporcionarán la información necesaria para mantener actualizado el sistema integral de seguimiento de contratación TIC que permita un análisis permanente de los contratos TIC.

Artículo 18. *Contenido del informe técnico sobre la memoria y los pliegos de prescripciones técnicas en materia de tecnologías de la información.*

1. El informe técnico de la memoria y de los pliegos de prescripciones técnicas en materia de tecnologías de la información se referirá a su adecuación a los planes estratégicos del departamento ministerial y a las directrices dictadas por la Dirección de Tecnologías de la Información y las Comunicaciones, así como a la finalidad y adecuación tecnológica de la prestación que se propone contratar.

2. El informe técnico tendrá en cuenta los elementos de la memoria y del pliego de prescripciones técnicas que contengan información relevante desde el punto de vista tecnológico y de los criterios para la transformación digital de los servicios.

Artículo 19. *Información presupuestaria.*

1. La Dirección de Tecnologías de la Información y las Comunicaciones tendrá información, en coordinación con las Comisiones Ministeriales de Administración Digital y la Dirección General de Presupuestos, de los recursos económicos destinados a los bienes y servicios TIC del conjunto de la Administración General del Estado y sus Organismos Públicos se informará trimestralmente a la Comisión de Estrategia TIC del estado de ejecución de dicho presupuesto.

2. La Dirección de Tecnologías de la Información y las Comunicaciones elaborará un informe anual detallado y desagregado de imputación de costes TIC.

Disposición adicional primera. *Supresión de órganos.*

A partir de la entrada en vigor de este real decreto quedan suprimidos el Consejo Superior de Administración Electrónica y las Comisiones Ministeriales de Administración Electrónica.

Disposición adicional segunda. *Modificación de referencias.*

1. Se entenderán referidas a la Comisión de Estrategia TIC y a las Comisiones Ministeriales de Administración Digital todas las alusiones que en la normativa vigente se hagan al Consejo Superior de Administración Electrónica y a las Comisiones Ministeriales de Administración Electrónica, respectivamente.

2. Sin perjuicio de lo anterior, todas las referencias al Consejo Superior de Administración Electrónica y a las Comisiones Ministeriales de Administración Electrónica que subsistan en la normativa vigente en relación a las competencias de contratación de estos órganos colegiados, se entenderán hechas a la Dirección de Tecnologías de la Información y las Comunicaciones.

3. Todos los comités técnicos, grupos de trabajo o ponencias especiales que hayan sido constituidos por acuerdo del Consejo Superior de Administración Electrónica o de su Comité Permanente quedarán asociados a la Dirección de Tecnologías de la Información y las Comunicaciones o a los órganos colegiados regulados en este real decreto, de acuerdo con sus funciones.

Disposición adicional tercera. *Régimen jurídico de los órganos colegiados.*

1. Los órganos colegiados que se regulan en este real decreto se regirán por lo establecido en materia de órganos colegiados en el capítulo II del título II de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

2. La Comisión de Estrategia TIC podrá aprobar las normas de régimen interno que estime procedentes para el mejor desarrollo de su trabajo.

Disposición adicional cuarta. *Representación del Ministerio de Defensa en los órganos con competencias en materia de Administración digital.*

Sin perjuicio de lo establecido en el artículo 5.1, la representación del Ministerio de Defensa en el Pleno de la Comisión de Estrategia TIC podrá ser asumida por el órgano superior de ese departamento que, de acuerdo con los reales decretos de estructura orgánica y de desarrollo de la misma, resulte competente en materia de Tecnologías de la Información y Comunicaciones.

Asimismo, sin perjuicio de lo establecido en el artículo 7.2, el citado órgano superior podrá asumir la presidencia de la Comisión Ministerial de Administración Digital del Ministerio de Defensa y, sin perjuicio de lo establecido en el artículo 8, podrá ser el responsable TIC, dentro de dicho órgano superior del Ministerio de Defensa, quien represente al departamento en el Comité de Dirección de las Tecnologías de Información y Comunicaciones.

Disposición adicional quinta. *Composición inicial del Comité Ejecutivo de la Comisión de Estrategia TIC.*

El Comité Ejecutivo de la Comisión de Estrategia TIC estará formado por los titulares de los siguientes órganos, en tanto que la Comisión de Estrategia TIC no establezca una composición diferente:

a) Dirección General de Racionalización y Centralización de la Contratación.
b) Dirección General de Presupuestos.
c) Dirección General de Telecomunicaciones y Tecnologías de la Información.
d) Gerencia de Informática de la Seguridad Social.
e) Departamento de Informática Tributaria de la Agencia Estatal de Administración Tributaria.
f) Secretaría General de la Administración de Justicia.
g) Dirección General de la Función Pública.
h) Inspección General del Ministerio de Hacienda y Administraciones Públicas.
i) Intervención General de la Administración del Estado.
j) Una Subdirección General del Centro Nacional de Inteligencia/Centro Criptológico Nacional.

Disposición adicional sexta. *Ámbito específico.*

Lo dispuesto en el presente real decreto será de aplicación a los organismos y entidades públicos no encuadrables en las categorías establecidas en el artículo 43.1 de la Ley 6/1997, de 14 de abril, de Organización y funcionamiento de la Administración General del Estado, en cuanto sea compatible con su normativa específica.

Disposición transitoria primera. *Expedientes de contratación en fase de informe.*

Se pospone hasta el 1 de enero de 2015 la entrada en vigor del nuevo procedimiento de tramitación de los informes de la memoria y de los pliegos de prescripciones técnicas.

Durante este periodo, los expedientes se seguirán tramitando por el procedimiento anterior, asumiendo directamente la Dirección de Tecnologías de la Información y las Comunicaciones la aprobación de los expedientes que hasta el momento eran competencia del Consejo Superior de Administración Electrónica.

Los expedientes que se inicien durante este periodo y los contratos adjudicados durante el mismo, así como los expedientes ya iniciados y los contratos adjudicados con anterioridad a la entrada en vigor de este real decreto se regirán de acuerdo con la normativa anterior. A estos efectos, se entenderá que los expedientes han sido iniciados cuando hayan sido remitidos a la Comisión Permanente del Consejo Superior de Administración Electrónica o a la correspondiente Comisión Ministerial de Administración Electrónica para su informe preceptivo o tramitación.

Disposición transitoria segunda. *Regulación de las Comisiones Ministeriales de Administración Digital.*

En el plazo de cuatro meses desde la entrada en vigor de este real decreto se aprobarán las correspondientes órdenes ministeriales reguladoras de las Comisiones Ministeriales de Administración Digital. Mientras tanto, subsistirán con su actual estructura las Comisiones Ministeriales de Administración Electrónica vigentes, que pasarán a ejercer las funciones que se atribuyen en este real decreto a las nuevas Comisiones Ministeriales de Administración Digital.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica, así como cuantas disposiciones de igual o inferior rango se opongan a lo establecido en este real decreto.

Disposición final primera. *Facultades de desarrollo.*

Se autoriza a los Ministros de Hacienda y Administraciones Públicas y de la Presidencia, en el ámbito de sus respectivas competencias, para que adopten las medidas necesarias para el desarrollo y ejecución de este real decreto.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 8

Orden HAP/1949/2014, de 13 de octubre, por la que se regula el Punto de Acceso General de la Administración General del Estado y se crea su sede electrónica

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 260, de 27 de octubre de 2014
Última modificación: 26 de noviembre de 2015
Referencia: BOE-A-2014-10908

En el marco de las reformas estructurales iniciadas por el Gobierno de la Nación, el pasado 26 de octubre de 2012 se acordó por el Consejo de Ministros la creación de una Comisión para la Reforma de las Administraciones Públicas (CORA) con el expreso objeto de realizar un estudio integral de la situación de las Administraciones Públicas en España y de proponer las reformas que sería necesario introducir en las mismas para dotarlas del tamaño, la eficiencia y la flexibilidad demandadas por los ciudadanos y la economía del país, y para transformar su estructura con vistas a posibilitar el crecimiento económico, la prestación efectiva de los servicios públicos y eliminar aquellas disfuncionalidades y defectos que pudieran dificultar ambos.

Entre otras medidas de reforma, CORA ha propuesto al Gobierno el establecimiento del Punto de Acceso General (PAG) como punto de entrada general, vía Internet, del ciudadano a las Administraciones Públicas. El fundamento de esta medida es la constatación de que en el momento actual existe una gran dispersión de la información de las Administraciones en distintos portales y páginas web, que provoca dificultades en el acceso de los ciudadanos a los procedimientos y servicios administrativos, informaciones duplicadas y falta de una coordinación adecuada en todas estas materias.

El PAG dispone de cobertura normativa en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, cuyo artículo 8 apartado 2, determina que la Administración General del Estado (AGE) contará con un sistema de varios canales o medios para garantizar a todos los ciudadanos la prestación de servicios electrónicos. Y en la letra b) de dicho apartado señala expresamente que, entre los puntos de acceso electrónico, se creará un Punto de Acceso General a través del cual, los ciudadanos puedan, en sus relaciones con la Administración General del Estado y sus Organismos Públicos, acceder a toda la información y a los servicios disponibles.

Por su parte, el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, tanto en su preámbulo, como en sus artículos 7, 8, 9, 24 y 31, define las características básicas que deberá tener el Punto y señala que habrá de contener la sede electrónica que, en este ámbito, facilita el acceso a los servicios, procedimientos e informaciones accesibles de la Administración General del Estado y de los organismos públicos vinculados o dependientes de la misma.

Las funciones principales del citado Punto, como posibilitar el acceso a la información y servicios de la Administración General del Estado, Comunidades Autónomas y Entidades

Locales, han venido realizándose parcialmente en los últimos años a través del sitio web Portal 060 (www.060.es), establecido en el ámbito de la Red 060 de Atención al Ciudadano, creada al amparo del Acuerdo de Consejo de Ministros de 15 julio de 2005 y, por ende, establecida con anterioridad a la propia ley 11/2007, de 22 de junio.

En ejecución de esta medida, y de las disposiciones normativas de la Ley 11/2007, de 22 de junio, y su Real Decreto de desarrollo, se dicta la presente orden, que tiene por finalidad la creación del PAG, la definición de su contenido y de su régimen de gobernanza y gestión, así como la creación de un fichero de datos de acuerdo con las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Adicionalmente, esta orden se dirige a crear la sede electrónica del PAG, en cumplimiento de las previsiones del Real Decreto 1671/2009, de 6 de noviembre.

La citada ley 11/2007, de 22 junio, estableció el concepto de sede electrónica, que define en el artículo 10, apartado 1, como aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a una Administración Pública, órgano o entidad administrativa en el ejercicio de sus competencias, señalando en el número 3 del mismo precepto que cada Administración Pública determinará las condiciones e instrumentos de creación de sus sedes electrónicas.

Por su parte, el Real Decreto 1671/2009, de 6 de noviembre, determina específicamente en su Título II, que las sedes electrónicas se crearán mediante orden del Ministro correspondiente o resolución del titular del organismo público, que deberá publicarse en el «Boletín Oficial del Estado», señalando el contenido mínimo de la misma.

La presente orden ha sido sometida al previo informe de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 37, párrafo h), de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y ha sido informada por la Comisión Permanente del Consejo Superior de Administración Electrónica.

En su virtud, a propuesta del Ministro de Hacienda y Administraciones Públicas, dispongo:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente orden tiene por objeto la regulación del Punto de Acceso General (en adelante PAG) y de su sede electrónica, así como la regulación del fichero de datos de carácter personal de la misma.

CAPÍTULO II

Punto de Acceso General

Artículo 2. *Alcance y características.*

1. El PAG, con los dominios www.administracion.es y www.administracion.gob.es, ofrecerá a los ciudadanos y empresas la información sobre los procedimientos y servicios de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes y reunirá la información de la actividad y la organización de las Administraciones Públicas.

2. El PAG contiene además el acceso a la sede electrónica asociada al mismo, de acuerdo con las características previstas en el artículo 7.

A este efecto, los Departamentos ministeriales y los Organismos públicos vinculados o dependientes deberán coordinar sus sedes electrónicas con la sede del PAG en los términos previstos en el artículo 5.

3. El PAG proporcionará información sobre los procedimientos y servicios correspondientes a otras Administraciones Públicas, mediante la formalización de los correspondientes instrumentos de colaboración.

4. Sin perjuicio de estos instrumentos, el acceso a procedimientos, servicios, e informaciones de las Administraciones Públicas, así como el intercambio de información entre ellas, se ajustará a lo previsto en los artículos 8 y 9 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5. Respecto a la coordinación del PAG con los portales electrónicos de los organismos internacionales y de las Administraciones Públicas extranjeras, especialmente de la Unión Europea y sus Estados miembros, se estará a lo dispuesto en la normativa correspondiente o a los convenios y acuerdos que pudieran existir. Las actuaciones de coordinación con los portales de la Unión Europea se canalizarán a través de la Representación Permanente de España en la misma.

Artículo 3. *Contenido y funcionalidades.*

1. El PAG deberá garantizar, de forma gradual y progresiva a medida que los recursos y desarrollos técnicos lo permitan, el acceso a los siguientes servicios:

a) Los portales de los Departamentos ministeriales y Organismos públicos vinculados o dependientes.

b) Su sede electrónica y las sedes electrónicas de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes.

c) Los servicios que la Administración pone a disposición de los ciudadanos y especialmente, los más usados por los ciudadanos.

d) Portal de transparencia.

e) Otros portales destacados de ámbito estatal como el portal de Datos abiertos, la Ventanilla Única de la Directiva de Servicios y aquellos de similar naturaleza.

f) Las áreas restringidas o privadas para los usuarios.

2. Además, el PAG contendrá información administrativa de carácter horizontal de los Departamentos ministeriales y Organismos públicos, vinculados o dependientes como las ayudas, becas, subvenciones, empleo público y legislación, que sean de interés para el ciudadano.

3. El PAG tendrá un espacio dedicado a la participación ciudadana y posibilitará la interactuación del ciudadano a través de las redes sociales más extendidas. También dispondrá de los mecanismos precisos que faciliten el acceso de sus contenidos a los diferentes dispositivos móviles existentes, a medida que los recursos y desarrollos técnicos lo permitan.

Artículo 4. *Acceso.*

Serán canales de acceso a los servicios del PAG:

1. Para el acceso electrónico, Internet, con las características definidas en el artículo 2.

2. Para la atención presencial, la oficina 060 de calle María de Molina, 50 (Madrid), así como las Oficinas 060 de Delegaciones y Subdelegaciones del Gobierno y de Direcciones Insulares, conforme a las competencias definidas en las normas reguladoras de la organización ministerial y el resto de las oficinas de las Administraciones Públicas en el marco de los convenios suscritos o que pudieran suscribirse, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

3. Para la atención telefónica, los servicios de información departamental, en el teléfono 060.

Artículo 5. *Titularidad y gestión.*

1. De acuerdo con lo regulado en el Real Decreto 1671/2009, de 6 de noviembre, la titularidad del PAG corresponderá al Ministerio de Hacienda y Administraciones Públicas, que establecerá los principios generales y directrices básicos de funcionamiento del mismo.

2. La gestión del PAG corresponde a la Dirección General de Organización Administrativa y Procedimientos que la ejercerá a través de la Subdirección General de la

Inspección General de Servicios de la Administración General del Estado y Atención al Ciudadano, en coordinación con la Dirección de Tecnologías de la Información y las Comunicaciones, de acuerdo con lo previsto en el artículo 16.1.e) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas.

3. Cada Departamento ministerial u Organismo público se responsabilizará de la provisión y actualización de la información que provea el portal en relación a sus procedimientos, servicios e informaciones a través de los mecanismos que se establezcan.

Artículo 6. *Gobernanza.*

1. Con el fin de garantizar una adecuada coordinación de la información contenida en el PAG y asegurar los necesarios niveles de colaboración para posibilitar la actualización permanente de la información y su adecuación a las demandas de los ciudadanos, se crea un Grupo de Trabajo, de acuerdo con lo dispuesto en el artículo 40.3 de la Ley 6/1997, de 14 de noviembre, de Organización y Funcionamiento de la Administración General del Estado, adscrito a la Dirección General de Organización Administrativa y Procedimientos. Este grupo contará con un representante de la Dirección de Tecnologías de la Información y las Comunicaciones así como con un representante por cada Departamento ministerial, al menos de nivel 30, que serán designados por la Subsecretaría de cada Departamento y que asumirán la representación de los Organismos públicos vinculados o dependientes del mismo.

2. Dicho Grupo de Trabajo tendrá atribuidas las siguientes funciones:

a) Potenciar la colaboración entre las unidades de información administrativa y/o unidades de gestión de sitios web de los distintos Departamentos ministeriales y de los Organismos públicos vinculados o dependientes a efectos de la actualización de la información contenida en el PAG.

b) Analizar los modelos de gobernanza que posibiliten una adecuada gestión y mantenimiento de la información.

c) Facilitar la coordinación y corresponsabilidad de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes respecto a la información contenida en el PAG.

d) Garantizar las acciones que se consideren convenientes para ofrecer un buen servicio de información administrativa y disponer de la información interdepartamental y de la que ofrezca cada Departamento ministerial y Organismo público vinculado o dependiente.

e) Colaborar en la gestión de la sede electrónica regulada en el Capítulo III de la presente orden.

3. Cada Departamento ministerial y Organismo público vinculado o dependiente a su vez se dotará de la estructura organizativa necesaria para garantizar la adecuada coordinación interna con el objeto de proveer los contenidos y sus actualizaciones en el PAG.

4. Sin perjuicio de lo establecido en su caso en los correspondientes instrumentos de colaboración, la participación y seguimiento de los contenidos del PAG referentes a otras Administraciones Públicas se verificarán a través del Comité Sectorial de Administración Electrónica.

CAPÍTULO III

Sede Electrónica del PAG

Artículo 7. *Creación y ámbito de aplicación.*

1. Se crea la sede electrónica del PAG, de acuerdo con lo dispuesto en los artículos 3 y 9 del Real Decreto 1671/2009, de 6 de noviembre.

2. El ámbito de aplicación de la sede comprenderá la totalidad de los Departamentos ministeriales y de los Organismos públicos vinculados o dependientes. Asimismo, la sede electrónica del PAG extenderá su ámbito a los organismos que se determinen en los instrumentos de colaboración con otras Administraciones Públicas que, en su caso, formalice

el Ministerio de Hacienda y Administraciones Públicas, al amparo de lo establecido en los artículos 3.3 y 9.1 del Real Decreto 1671/2009, de 6 de noviembre.

3. Esta sede se considerará como la sede central de la Administración General del Estado.

Artículo 8. *Características.*

1. A través de la sede electrónica del PAG se podrá acceder a los procedimientos y servicios que requieran la autenticación de los ciudadanos o de la Administración Pública en sus relaciones con éstos por medios electrónicos, así como aquellos otros respecto a los que se decida su inclusión en la sede por razones de eficacia y calidad en la prestación de servicios a los ciudadanos y que estén accesibles en las sedes electrónicas de los órganos correspondientes. A medida que los recursos y desarrollos técnicos lo permitan, este acceso se podrá realizar sin tener que identificarse de nuevo.

2. La dirección electrónica de referencia de la sede será:

https://sede.administracion.gob.es.

3. Los servicios incluidos en la sede electrónica del PAG cumplirán los principios de accesibilidad y usabilidad, establecidos en la Ley 11/2007, de 22 de junio, así como en los términos dictados por la normativa vigente en esta materia en cada momento.

4. Los contenidos publicados en la sede electrónica del PAG responderán a los criterios de seguridad e interoperabilidad según lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y por el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5. Serán canales de acceso a los servicios disponibles en la sede:

a) Para el acceso electrónico, Internet, con las características definidas en el presente artículo.

b) Para la atención presencial, la oficina 060 de calle María de Molina, 50 (Madrid), así como las Oficinas 060 de Delegaciones y Subdelegaciones del Gobierno y de Direcciones Insulares, conforme a las competencias definidas en las normas reguladoras de la organización ministerial, sin perjuicio del acceso a través de los registros regulados en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

c) Para la atención telefónica, los servicios de información departamental, en el teléfono 060.

Artículo 9. *Contenidos.*

1. La sede electrónica del PAG dispondrá del contenido mínimo y de los servicios previstos expresamente en los apartados 1 y 2 del artículo 6 del Real Decreto 1671/2009, de 6 de noviembre.

2. Además la sede electrónica del PAG dispondrá de los siguientes contenidos específicos:

a) Acceso a Trámites y Servicios en línea disponibles en las sedes electrónicas.

b) Registro Electrónico Común.

c) Dirección Electrónica Habilitada.

d) Registro Electrónico de Apoderamientos.

e) Registro de Funcionarios Habilitados.

f) Servicios que requieran de autenticación de la administración y/o del ciudadano como la inscripción en pruebas selectivas, cambio de domicilio y notificaciones electrónicas, entre otros.

g) Enlace a la orden de creación, publicada en el Boletín Oficial del Estado.

h) Buzón de contacto del PAG.

i) Cualquier otro contenido de interés para el ciudadano que deba figurar en la Sede Electrónica del PAG.

3. A medida que los recursos y desarrollos técnicos lo permitan, la Sede Electrónica del PAG posibilitará el acceso a sus contenidos en lenguas cooficiales.

Artículo 10. *Titularidad y gestión de la sede electrónica del PAG.*

1. La titularidad de la Sede Electrónica del PAG corresponderá al Ministerio de Hacienda y Administraciones Públicas en los mismos términos previstos en el artículo 5.1.

2. La gestión de la sede corresponde a la Dirección General de Organización Administrativa y Procedimientos que la ejercerá a través de la Subdirección General de la Inspección General de Servicios de la Administración General del Estado y Atención al Ciudadano, en coordinación con la Dirección de Tecnologías de la Información y las Comunicaciones, de acuerdo con lo previsto en el artículo 16.1 e) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas.

3. Los Departamentos ministeriales y los Organismos públicos vinculados o dependientes de los mismos participarán en la gestión de la sede electrónica del PAG a través del mecanismo previsto en el artículo 6.

4. Sin perjuicio de lo establecido en su caso en los correspondientes instrumentos de colaboración, la participación y seguimiento de los contenidos de la sede electrónica del PAG referentes a otras Administraciones Públicas, se verificarán a través del Comité Sectorial de Administración Electrónica.

5. El titular de la sede electrónica del PAG será responsable de la integridad, veracidad y actualización de la información y servicios a los que pueda accederse a través de la misma. En el caso de los enlaces o vínculos cuya responsabilidad corresponde a distinto órgano o Administración Pública, el titular de la sede electrónica del PAG no será responsable de la integridad, veracidad ni actualización de aquéllos.

Artículo 11. *Medios para la formulación de quejas y sugerencias.*

1. Los medios disponibles para la formulación de quejas y sugerencias en relación con el contenido, gestión y servicios ofrecidos en la sede que se crea en la presente orden y sin perjuicio de los procedimientos específicos, serán los siguientes:

a) Presentación presencial o por correo postal ante los registros y las oficinas de atención al público de los servicios centrales y de las oficinas periféricas del Ministerio de Hacienda y Administraciones Públicas, así como en los lugares previstos en el artículo 38.4 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y Procedimiento Administrativo Común, dirigidas a los órganos u organismos responsables, y de acuerdo con lo dispuesto en el artículo 9 y según el procedimiento establecido en capítulo IV del Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

b) Presentación electrónica a través del Servicio electrónico de quejas y sugerencias de la Inspección General del Ministerio de Hacienda y Administraciones Públicas, enlazado en la Sede electrónica del PAG así como de aquellos medios que prevé la Ley 11/2007, de 22 de junio.

2. No se considerarán medios para la formulación de quejas y sugerencias los servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede, sin perjuicio de su obligación, cuando existan, de atender las cuestiones que susciten los ciudadanos.

Disposición adicional primera. *Régimen económico.*

Las medidas contenidas en esta orden se cumplirán con los medios presupuestarios, personales y materiales existentes en cada Departamento ministerial u Organismo público vinculado o dependiente responsable de la información que provea el PAG y en ningún caso podrá generar incremento de gasto público.

Disposición adicional segunda. *Referencias al portal 060.*

Las referencias al portal 060 que se contengan en cualquier Convenio de colaboración suscrito para la implantación de oficinas integradas se entenderán realizadas al PAG.

Disposición transitoria única. *Portal 060 y Sede 060.*

El portal 060 (www.060.es) y su sede (https://sede.060.gob.es) seguirán en funcionamiento hasta la puesta en marcha del PAG.

Disposición final primera. *Desarrollo.*

Se autoriza al Secretario de Estado de Administraciones Públicas a dictar las instrucciones precisas para el cumplimiento de la presente orden.

Disposición final segunda. *Modificación de la Orden HAP 2478/2013, de 20 de diciembre, por la que se regulan los ficheros de datos de carácter personal existentes en el departamento y en determinados organismos adscritos al mismo.*

1. En cumplimiento de lo previsto en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, se crea el fichero de datos personales «Sede electrónica del Punto de Acceso General», cuya titularidad corresponde a la Dirección General de Organización Administrativa y Procedimientos, situada en calle María de Molina, número 50, 28071, Madrid, válido a efectos del ejercicio por parte de los ciudadanos de los derechos previstos por dicha ley.

2. El contenido del fichero se recoge en el anexo de la presente orden.

3. Dicho fichero se añade a los ficheros de la Dirección General de Organización Administrativa y Procedimientos del Ministerio de Hacienda y Administraciones Públicas que se recogen en la Orden ministerial HAP 2478/2013, de 20 de diciembre, por la que se regulan los ficheros de datos de carácter personal existentes en el departamento y en determinados organismos públicos adscritos al mismo.

Disposición final tercera. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Fichero de datos personales

(Suprimido)

§ 9

Resolución de 7 de julio de 2021, de la Secretaría General de Administración Digital, por la que se aprueba la Política de Seguridad de los servicios prestados por la Secretaría General de Administración Digital

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 172, de 20 de julio de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-12148

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas regula en su artículo 13 los derechos de las personas en sus relaciones con las Administraciones Públicas, incluyendo en su apartado h) el relativo a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, al regular en su artículo 3 los principios generales que las Administraciones Públicas deben respetar en su actuación y relaciones, establece en su apartado 2 que aquellas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.

En el artículo 156.2 de la misma norma prevé la existencia del Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

El Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica se regula en el Real Decreto 3/2010, de 8 de enero, cuyo artículo 11.1 establece el mandato de que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad aprobada por su titular, que articule la gestión continuada de la seguridad. Dicha política de seguridad se establecerá de acuerdo con los principios básicos que recogen los artículos 4 a 10 y se desarrollará aplicando los requisitos mínimos que detalla el propio artículo 11.1.

El anexo II del real decreto, al regular las medidas de seguridad, incluye el marco organizativo entre el primer grupo de dichas medidas, que comprende, entre otras, la política de seguridad. Al respecto, el apartado 3.1 del Anexo II establece que la política de seguridad debe referenciar y ser coherente con lo establecido en la legislación de protección de datos de carácter personal, en lo que corresponda, en particular, por el Reglamento UE 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo

que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y por lo previsto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

El Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital en el artículo 9 atribuye a la Secretaría General de Administración Digital (en adelante, SGAD), un amplio conjunto de competencias de carácter transversal a toda la Administración General del Estado y sus Organismos Públicos, entre ellas la provisión de servicios en materia de tecnologías de la información y comunicaciones y la prestación de aplicaciones y servicios para Delegaciones y Subdelegaciones del Gobierno y las Direcciones Insulares en todos sus ámbitos de actuación, en materia de tecnologías de la información y comunicaciones.

A la luz de las competencias previstas en el artículo 9 del Real Decreto 403/2020, de 25 de febrero, y en coherencia con la estrategia de racionalización encomendada a la Secretaría General de Administración Digital, la presente resolución tiene como finalidad aprobar la Política de Seguridad única en el ámbito de todos los servicios de tecnologías de la información prestados por la Secretaría General de Administración Digital, independientemente de la adscripción orgánica de la Unidad destinataria de los mismos. Asimismo, la resolución establece la estructura organizativa necesaria para desarrollar, implantar y gestionar esta política.

En virtud de lo anterior, en cumplimiento del artículo 11 del Real Decreto 3/2010, de 8 de enero, previo informe de la Abogacía del Estado, dispongo:

Primero.

Se aprueba la «Política de Seguridad de los servicios prestados por la Secretaría General de Administración Digital», cuyo texto se incluye a continuación.

Segundo.

La Política de seguridad de los servicios prestados por la Secretaría General de Administración Digital se aplicará desde el día siguiente al de la publicación de la presente Resolución en el «Boletín Oficial del Estado».

POLÍTICA DE SEGURIDAD DE LOS SERVICIOS PRESTADOS POR LA SECRETARÍA GENERAL DE ADMINISTRACIÓN DIGITAL

Artículo 1. *Objeto.*

1. La Política de Seguridad de los servicios prestados por la Secretaría General de Administración Digital (en adelante, SGAD) tiene por objeto identificar responsabilidades y establecer principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por la Secretaría General de Administración Digital mediante las tecnologías de la información y de las comunicaciones, así como la estructuración de la correspondiente documentación de seguridad.

2. La Política de Seguridad es el instrumento en el que se apoya la Secretaría General de Administración Digital para garantizar el uso seguro de los sistemas de información y las comunicaciones, en el ejercicio de las competencias, previstas en el artículo 9 del Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital.

Artículo 2. *Misión y funciones de la Secretaría General de Administración Digital.*

Sin perjuicio del resto de competencias previstas en el artículo 9 del Real Decreto 403/2020, de 25 de febrero, las competencias de la Secretaría General de Administración Digital relativas a la prestación de servicios se encuadran en los siguientes ejes de actuación:

a) Prestación de Servicios TIC comunes y de carácter horizontal, incluidos los servicios declarados compartidos por la Comisión de Estrategia TIC en su reunión de 15 de septiembre de 2015, u otros que puedan ser declarados con posterioridad.

b) Prestación de Servicios TIC sectoriales, tanto los prestados por la Secretaría General de Administración Digital en virtud de sus competencias como los prestados a aquellos órganos, unidades, organismos y entes públicos con los que se acuerde la provisión.

c) Prestación de servicios directos a ciudadanos y empresas.

Artículo 3. *Principios rectores de la Política de Seguridad.*

Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el Esquema Nacional de Seguridad regulado por el Real Decreto 3/2010, de 8 de enero, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo.

Artículo 4. *Desarrollo normativo.*

1. El cuerpo normativo sobre seguridad de la información es de obligado cumplimiento y se desarrollará en tres niveles, de manera que cada norma de un determinado nivel de desarrollo se fundamente en las normas de nivel superior. Dichos niveles de desarrollo normativo son los siguientes:

a) Primer nivel normativo: constituido por la presente Política de Seguridad.

b) Segundo nivel normativo: constituido principalmente por las normas y directrices de seguridad generales que, respetando lo estipulado por la Política de Seguridad, determinan qué se puede hacer y qué no desde el punto de vista de la seguridad en relación con los servicios prestados por la Secretaría General de Administración Digital, sin considerar aspectos relativos a implementación ni tecnológicos.

La documentación perteneciente a este segundo nivel normativo será aprobada por Resolución del Secretario General de Administración Digital a propuesta del Responsable de Seguridad, previo acuerdo en el Grupo de Trabajo de Seguridad de los servicios prestados por la Secretaría General de Administración Digital.

c) Tercer nivel normativo: constituido por políticas específicas que, respetando lo dispuesto en los niveles normativos anteriores, apliquen a ámbitos o sistemas de información particulares. También estará constituido por procedimientos, guías e instrucciones de carácter técnico o procedimental.

La documentación perteneciente a este tercer nivel normativo será aprobada por el Responsable de Seguridad, previo acuerdo en el Grupo de Trabajo de Seguridad de los servicios prestados por la Secretaría General de Administración Digital.

2. El Responsable de Seguridad será el encargado de mantener la documentación de seguridad actualizada y organizada, y de gestionar los mecanismos de acceso a la misma.

3. El personal de cada uno de los órganos u organismos a los que es de aplicación la presente Política de Seguridad tendrá la obligación de conocerla y cumplirla y las normas y procedimientos de seguridad de la información que puedan afectar a sus funciones. A tal efecto, la Secretaría General de Administración Digital pondrá a disposición de todas las entidades usuarias de sus servicios la documentación pertinente.

Artículo 5. *Estructura organizativa.*

1. La organización de la seguridad tendrá en cuenta la organización propia de la Secretaría General de Administración Digital y la de los órganos, organismos y entidades usuarios de sus servicios. En consecuencia, deberá garantizarse la actuación coordinada y eficaz, según lo establecido al respecto en el Esquema Nacional de Seguridad y en las orientaciones de la guía CCN-STIC 801 ‘Responsabilidades y funciones’.

2. Sin perjuicio de lo anterior, son órganos que intervienen en el desarrollo de la presente Política de Seguridad:

a) El Secretario General de Administración Digital.

b) El Grupo de trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital.

c) El Responsable de Seguridad.
d) El Responsable del Sistema.
e) Los Responsables de la Información.
f) Los Responsables del Servicio.
g) Los Delegados de Protección de Datos

3. Los órganos u organismos sujetos a la presente Política de Seguridad deberán disponer de la estructura organizativa necesaria para cumplir adecuadamente con sus obligaciones en el ámbito de los servicios que presta la Secretaría General de Administración Digital.

Artículo 6. *Competencias del Secretario General de Administración Digital.*

La persona titular de la Secretaría General de Administración Digital es, en el ejercicio de sus competencias, el responsable del funcionamiento de los servicios que presta la Secretaría General de Administración Digital. En particular:

a) Coordinará todas las actividades relacionadas con la seguridad de los servicios prestados por la Secretaría General de Administración Digital, tanto de carácter horizontal, común o compartido, como de carácter sectorial.
b) Impulsará la adecuación a la normativa aplicable de seguridad de la información y de protección de datos, dentro de su ámbito de competencias.
c) Será responsable de la modificación y actualización de esta Política de Seguridad, así como de aprobar las normas de seguridad propuestas por el Responsable de Seguridad, previo acuerdo del Grupo de Trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital.

Artículo 7. *Grupo de trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital.*

1. Con carácter permanente, se crea el Grupo de trabajo de seguridad de los servicios prestados por la Secretaría General de Administración Digital (en adelante, GTS) como órgano de asesoramiento del Secretario General de Administración Digital en materia de seguridad.
El GTS estará compuesto por:

a) Presidente: el Responsable de Seguridad de la Secretaría General de Administración Digital.
b) Vicepresidente: el Responsable del Sistema de la Secretaría General de Administración Digital.
c) Un vocal de cada una de las siguientes unidades de la Secretaría General de Administración Digital designado por el titular respectivo:

1.º La División de Planificación y Coordinación de Ciberseguridad.
2.º La Subdirección General de Planificación y Gobernanza de la Administración Digital.
3.º La Subdirección General de Impulso de la Digitalización de la Administración.
4.º La Subdirección General de Infraestructuras y Operaciones.
5.º La Subdirección General de Servicios Digitales para la Gestión.
6.º La Subdirección General de Presupuestos y Contratación TIC.
7.º El Gabinete de la Secretaría General de Administración Digital.

d) Secretario: un funcionario de la División de Planificación y Coordinación de Ciberseguridad, nombrado por su titular, que actuará con voz pero sin voto.

2. Cada unidad representada en el GTS podrá convocar a personal en calidad de asesor, con voz, pero sin voto.
3. El Presidente podrá convocar, en razón de los asuntos tratados, a representantes de cualquier órgano y unidad que accedan a sistemas de información de la Secretaría General de Administración Digital, así como a expertos tanto de la Secretaría General de Administración Digital como de otras entidades.
4. El GTS llevará a cabo las siguientes funciones:

a) Elaborar estudios, análisis y propuestas de modificación y actualización de la Política de Seguridad y de la normativa de la seguridad de la información de segundo y tercer nivel.

b) Solicitar al Responsable de Seguridad la toma en consideración de cualquier aspecto que considere relevante respecto a la seguridad de la información.

c) Velar por la coherencia y armonización de la normativa y actuaciones en materia de seguridad de la información entre los distintos servicios ofrecidos por la Secretaría General de Administración Digital, ya sean los de carácter común, horizontal o sectorial.

d) Asesorar al Responsable de Seguridad en la preparación o confección de la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

e) Estudiar y proponer actividades de concienciación y formación en materia de seguridad.

f) Realizar cualquier otra actividad de asesoría, formulación de recomendaciones, o propuesta de iniciativas, en materia de seguridad.

g) Cualquier otra función en el ámbito de la seguridad de la información y los servicios que le encomiende el Secretario General de Administración Digital.

5. El GTS se reunirá al menos una vez al cuatrimestre y sus decisiones se adoptarán por mayoría de sus miembros con derecho a voto.

Artículo 8. *Responsable de Seguridad.*

1. El Director de la División de Planificación y Coordinación de Ciberseguridad, en su condición de Responsable de Seguridad en el ámbito de la presente Política de Seguridad, es la persona que determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, de acuerdo con lo previsto en el artículo 10 del Real Decreto 3/2010, de 8 de enero.

2. El ámbito de actuación del Responsable de Seguridad se extiende a todos los servicios prestados por la Secretaría General de Administración Digital, debiendo velar por la coherencia y armonización de las normas, procedimientos y actuaciones de la Secretaría General de Administración Digital en los diferentes ámbitos.

3. Son funciones específicas del Responsable de Seguridad:

a) Promover la seguridad de los servicios prestados por la Secretaría General de Administración Digital y la mejora continua en su gestión.

b) Proponer al SGAD, previo acuerdo del GTS, la aprobación de la normativa de seguridad de segundo nivel.

c) Aprobar la normativa de seguridad de tercer nivel, previo acuerdo del GTS.

d) Impulsar y velar por el cumplimiento y difusión de la Política de Seguridad y de su cuerpo normativo, promoviendo las actividades de concienciación y formación en materia de seguridad para todo el personal afectado por la Política de Seguridad.

e) Asesorar, en colaboración con el Responsable del Sistema, a los Responsables de la Información y Responsables del Servicio, en la realización de los preceptivos análisis de riesgos.

f) Determinar, junto con el Responsable del Sistema, la agrupación en sistemas de los servicios TIC prestados por la Secretaría General de Administración Digital, y la categoría de estos sistemas, según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero; y determinar las medidas de seguridad que deben aplicarse, de acuerdo con lo previsto en el anexo II del Real Decreto 3/2010, de 8 de enero.

g) Aprobar la Declaración de Aplicabilidad, que comprende la relación de medidas de seguridad seleccionadas para un sistema.

h) Promover auditorías periódicas para verificar el cumplimiento de las obligaciones en materia de seguridad de la información, y analizar los informes fruto de las mismas.

i) Proponer las decisiones respecto a medidas de contingencia que considere imprescindibles para preservar la seguridad de los servicios prestados por la Secretaría General de Administración Digital.

j) Informar periódicamente al SGAD sobre el estado de la seguridad en el ámbito de esta Política de Seguridad. Para ello podrá utilizar informes de incidentes de seguridad, resultados de auditorías y análisis de riesgos realizados, y, en general, cualquier información

de seguridad relevante que pueda recabar en el desarrollo de sus funciones, o a través de solicitud al GTS.

k) Realizar cualquier otra actividad relativa a la seguridad de los servicios prestados por la Secretaría General de Administración Digital.

4. El Responsable de Seguridad podrá designar motivadamente, siendo responsable de su actuación, los Responsables de Seguridad Delegados que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

Artículo 9. *Responsable del Sistema.*

1. El Responsable del Sistema, nombrado por el Secretario General de Administración Digital, tiene la responsabilidad de desarrollar, operar y mantener el sistema de información que soporta los distintos servicios, durante todo su ciclo de vida.

Su ámbito de actuación se extenderá a todos los sistemas que sustentan servicios prestados por la Secretaría General de Administración Digital, con independencia de su naturaleza.

2. Son funciones del Responsable del Sistema:

a) Implantar las medidas necesarias para garantizar la seguridad del servicio durante todo su ciclo de vida, contando con el asesoramiento del Responsable de Seguridad del ámbito de competencia correspondiente.

b) Aprobar toda modificación sustancial de la configuración de cualquier elemento del sistema.

c) Asesorar, en colaboración con el Responsable de Seguridad, a los Responsables de la Información y a los Responsables del Servicio en la realización de los preceptivos análisis de riesgos.

d) Determinar, junto con el Responsable de Seguridad, la agrupación de los servicios TIC prestados por la Secretaría General de Administración Digital en sistemas, y la categoría de estos sistemas, según el procedimiento descrito en el anexo I del Real Decreto 3/2010, de 8 de enero.

e) Suspender el manejo de una determinada información o la prestación de un servicio electrónico si es informado o detecta deficiencias graves de seguridad, previo acuerdo con el Responsable de dicha información o servicio, y con el Responsable de Seguridad.

3. El Responsable del Sistema deberá coordinar las actuaciones de interconexión y acceso a los servicios de la Secretaría General de Administración Digital con los responsables del sistema de los organismos o entidades a los que la Secretaría General de Administración Digital preste sus servicios, bajo las directrices establecidas por el cuerpo normativo de seguridad.

4. El Responsable del Sistema podrá designar motivadamente, siendo responsable de su actuación, los Responsables de Sistema Delegados que considere necesarios para el adecuado cumplimiento de sus funciones, quienes actuarán bajo su coordinación y de acuerdo con sus criterios.

Artículo 10. *Responsables de la Información y Responsables del Servicio.*

1. De acuerdo con lo previsto en el artículo 10 del Real Decreto 3/2010, de 8 de enero, y en la correspondiente guía CCN-STIC sobre roles y funciones en el ENS, en los sistemas de información el responsable de la información determinará los requisitos de la información tratada y el responsable del servicio determinará los requisitos de los servicios prestados.

2. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos.

3. Dado que la Secretaría General de Administración Digital ofrece servicios a otras entidades, incluidos servicios sectoriales y servicios horizontales, comunes y compartidos a otras entidades, los Responsables de la Información o del Servicio pertenecerán en general a esas otras entidades, que nombrarán a los citados responsables y los comunicarán al SGAD. El modelo de relación con estos representantes lo establecerá la Secretaría General de Administración Digital conforme al modelo de prestación de cada servicio.

4. En caso de que un servicio prestado por un sistema de información de la Secretaría General de Administración Digital se realice en la nube, en modo multicliente, y dicho servicio no tenga Responsables de la Información o del Servicio nombrados, la Secretaría General de Administración Digital podrá asumir las funciones de Responsable de la Información o del Servicio en el ámbito de dicho sistema de información.

5. Los Responsables de la Información o del Servicio asistirán, conforme a lo dispuesto en el artículo 7 de esta Política de Seguridad, a las reuniones del GTS de los servicios prestados por la Secretaría General de Administración Digital, cuando sean requeridos por su Presidente.

6. Las funciones de cada Responsable de Información y Responsable del Servicio, dentro de su ámbito de actuación y con el asesoramiento y colaboración del Responsable de Seguridad y el Responsable del Sistema serán las siguientes:

a) Determinar los niveles de seguridad de la información tratada y de los servicios prestados, respectivamente.

b) Realizar, con el asesoramiento del Responsable de Seguridad y del Responsable del Sistema, los preceptivos análisis de riesgos y auditorías de seguridad, acordando con dichos responsables las salvaguardas a implantar.

c) Aceptar los riesgos residuales calculados en el análisis de riesgos.

Artículo 11. *Delegados de Protección de Datos.*

Los Delegados de Protección de Datos desempeñarán, cuando la Secretaría General de Administración Digital sea Encargada del tratamiento, y dentro de su ámbito de actuación y de sus competencias, las funciones del Delegado de Protección de Datos indicadas en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de Abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás disposiciones reguladoras de la materia.

Artículo 12. *Resolución de conflictos.*

En caso de conflicto entre los diferentes responsables, éste será resuelto por su superior jerárquico, si pertenecen al mismo órgano superior. En su defecto resolverá el Secretario General de Administración Digital.

§ 10

Ley 22/2021, de 28 de diciembre, de Presupuestos Generales del Estado para el año 2022. [Inclusión parcial]

Jefatura del Estado
«BOE» núm. 312, de 29 de diciembre de 2021
Última modificación: 24 de diciembre de 2022
Referencia: BOE-A-2021-21653

[. . .]

Disposición adicional centésima décima séptima. *Creación de la Agencia Estatal de Administración Digital.*

Uno. De acuerdo con lo previsto en el artículo 91 de la Ley 40/2015, de 1 de octubre, del Régimen Jurídico del Sector Público, se autoriza la creación de la Agencia Estatal de Administración Digital, como organismo público con personalidad jurídica pública y patrimonio propios y plena capacidad de obrar.

Dos. La actuación de la Agencia responderá a los siguientes fines:

a) La digitalización del sector público, mediante el ejercicio de las funciones de dirección, coordinación y ejecución del proceso de transformación digital e innovación de la Administración a través de las tecnologías de la información y de las comunicaciones.

b) La prestación eficiente de los servicios públicos, a través de la adopción de soluciones digitales, en el marco de los Esquemas Nacionales de Seguridad e Interoperabilidad.

c) La transformación digital de las Administraciones Públicas a través de la coordinación de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, y de la cooperación con las administraciones públicas para la implantación de las estrategias nacionales e internacionales en materia de administración digital.

d) La coordinación funcional de la actuación de las unidades TIC de la Administración General del Estado y el apoyo informático a aquellos departamentos ministeriales que lo precisen.

Tres. De acuerdo con los fines enunciados, corresponderá a la Agencia el impulso en la definición, desarrollo, ejecución y seguimiento, entre otros, de los proyectos de transformación digital incluidos el Plan de Digitalización de las Administraciones Públicas 2021-2025 para mejorar la accesibilidad de los servicios públicos digitales a la ciudadanía y empresas, superar la actual brecha digital y favorecer la eficiencia y eficacia de los empleados públicos, avanzando hacia una Administración del siglo XXI y contribuyendo a la consecución de objetivos de resiliencia y transición digital perseguidos también por el Plan Nacional de Recuperación, Transformación y Resiliencia.

Esto se llevará a cabo mediante la ejecución, entre otras actuaciones, de las medidas incluidas en el Plan de Digitalización de las Administraciones Públicas 2021-2025.

Cuatro. Estará adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital. Se regirá por lo establecido en su estatuto orgánico y por lo dispuesto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Cinco. La asistencia jurídica, consistente en el asesoramiento y la representación y defensa en juicio de la Agencia, corresponderá a los Abogados del Estado integrados en el Servicio Jurídico del Estado.

[. . .]

§ 11

Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

Jefatura del Estado
«BOE» núm. 298, de 12 de noviembre de 2020
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2020-14046

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

Desde el 1 de julio de 2016 es de aplicación el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

La Ley 59/2003, de 19 de diciembre, de firma electrónica, que supuso la transposición al ordenamiento jurídico español de la derogada Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, se encuentra desde entonces jurídicamente desplazada en todo aquello regulado por el citado Reglamento. El objeto de esta Ley es, por tanto, adaptar nuestro ordenamiento jurídico al marco regulatorio de la Unión Europea, evitando así la existencia de vacíos normativos susceptibles de dar lugar a situaciones de inseguridad jurídica en la prestación de servicios electrónicos de confianza.

La presente Ley no realiza una regulación sistemática de los servicios electrónicos de confianza, que ya han sido legislados por el Reglamento (UE) 910/2014, el cual, por respeto al principio de primacía del Derecho de la Unión Europea, no debe reproducirse total o parcialmente. La función de esta Ley es complementarlo en aquellos aspectos concretos que el Reglamento no ha armonizado y cuyo desarrollo prevé en los ordenamientos de los diferentes Estados miembros, cuyas disposiciones han de ser interpretadas de acuerdo con él.

II

En lugar de una revisión de la Directiva 1999/93/CE, la elección de un reglamento como instrumento legislativo por el legislador europeo, de aplicación directa en los Estados miembros, vino motivada por la necesidad de reforzar la seguridad jurídica en el seno de la Unión, terminando con la dispersión normativa provocada por las transposiciones de la citada Directiva en los ordenamientos jurídicos internos a través de leyes nacionales, que había provocado una importante fragmentación e imposibilitado la prestación de servicios transfronterizos en el mercado interior, agravada por las diferencias en los sistemas de supervisión aplicados en cada Estado miembro.

Así, mediante el Reglamento (UE) 910/2014 se persigue regular en un mismo instrumento normativo de aplicación directa en los Estados miembros dos realidades, la identificación y los servicios de confianza electrónicos en sentido amplio, armonizando y facilitando el uso transfronterizo de los servicios en línea, públicos y privados, así como el comercio electrónico en la UE, contribuyendo así al desarrollo del mercado único digital.

Por una parte, en el ámbito de la identificación electrónica, el Reglamento instaura la aceptación mutua, para el acceso a los servicios públicos en línea, de los sistemas nacionales de identificación electrónica que hayan sido notificados a la Comisión Europea por parte de los Estados miembros, con objeto de facilitar la interacción telemática segura con las Administraciones públicas y su utilización para la realización de trámites transfronterizos, eliminando esta barrera electrónica que excluía a los ciudadanos del pleno disfrute de los beneficios del mercado interior.

Por otra parte, introduce la regulación armónica de nuevos servicios electrónicos cualificados de confianza, adicionales a la tradicional firma electrónica, tales como el sello electrónico de persona jurídica, el servicio de validación de firmas y sellos cualificados, el servicio de conservación de firmas y sellos cualificados, el servicio de sellado electrónico de tiempo, el servicio de entrega electrónica certificada y el servicio de expedición de certificados de autenticación web, que pueden ser combinados entre sí para la prestación de servicios complejos e innovadores.

Se establece un régimen jurídico específico para los citados servicios electrónicos de confianza cualificados, consecuente con las elevadas exigencias de supervisión y seguridad que soportan, y cuyo reflejo es la singular relevancia probatoria que poseen respecto de los servicios no cualificados. Se refuerza así la seguridad jurídica de las transacciones electrónicas entre empresas, particulares y Administraciones públicas.

III

La aplicabilidad directa del Reglamento no priva a los Estados miembros de toda capacidad normativa sobre la materia regulada, es más, aquellos están obligados a adaptar los ordenamientos nacionales para garantizar que aquella cualidad se haga efectiva. Esta adaptación puede exigir tanto la modificación o derogación de normas existentes, como la adopción de nuevas disposiciones llamadas a completar la regulación europea.

En tal sentido, el objetivo de la presente Ley, como se indicaba ut supra, es complementar el Reglamento (UE) 910/2014 en aquellos aspectos que este no ha armonizado y que se dejan al criterio de los Estados miembros. Por tanto, la Ley se abstiene de reproducir las previsiones del Reglamento, abordando únicamente aquellas cuestiones que la norma europea remite a la decisión de los Estados miembros o que no se encuentran armonizadas, adquiriendo la regulación coherencia y sentido en el marco de la normativa europea.

Así, en virtud del principio de proporcionalidad, esta Ley contiene la regulación imprescindible para cubrir aquellos aspectos previstos en el Reglamento (UE) 910/2014, como es el caso, entre otros, del régimen de previsión de riesgo de los prestadores cualificados, el régimen sancionador, la comprobación de la identidad y atributos de los solicitantes de un certificado cualificado, la inclusión de requisitos adicionales a nivel nacional para certificados cualificados tales como identificadores nacionales, o su tiempo máximo de vigencia, así como las condiciones para la suspensión de los certificados.

El Reglamento (UE) 910/2014 garantiza la equivalencia jurídica entre la firma electrónica cualificada y la firma manuscrita, pero permite a los Estados miembros determinar los

efectos de las otras firmas electrónicas y de los servicios electrónicos de confianza en general. En este aspecto, se modifica la regulación anterior al atribuir a los documentos electrónicos para cuya producción o comunicación se haya utilizado un servicio de confianza cualificado una ventaja probatoria. A este respecto, se simplifica la prueba, pues basta la mera constatación de la inclusión del citado servicio en la lista de confianza de prestadores cualificados de servicios electrónicos regulada en el artículo 22 del Reglamento (UE) 910/2014.

Por lo que respecta a los certificados electrónicos, se introducen en la Ley varias disposiciones relativas a la expedición y contenido de los certificados cualificados, cuyo tiempo máximo de vigencia se mantiene en cinco años. En este sentido, no se permite a los prestadores de servicios el denominado «encadenamiento» en la renovación de certificados cualificados utilizando uno vigente, más que una sola vez, por razones de seguridad en el tráfico jurídico. Sin perjuicio de lo anterior, el Reglamento (UE) 910/2014 contempla la posibilidad de verificación de la identidad del solicitante de un certificado cualificado utilizando otros métodos de identificación reconocidos a escala nacional que garanticen una seguridad equivalente en términos de fiabilidad a la presencia física. Haciéndose eco de esta previsión, la Ley habilita a que reglamentariamente se regulen las condiciones y requisitos técnicos que lo harían posible.

Los certificados cualificados expedidos a personas físicas incluirán el número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, salvo en los casos en los que el titular carezca de todos ellos. La misma regla se aplica en cuanto al número de identificación fiscal de las personas jurídicas o sin personalidad jurídica titulares de certificados cualificados, que en defecto de este han de utilizar un código que les identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

En lo que se refiere a las obligaciones de los prestadores, la Ley establece el requisito de constitución de una garantía económica para la prestación de servicios cualificados de confianza. Se fija una cuantía mínima única de 1.500.000 euros, que se incrementa en 500.000 euros por cada tipo de servicio adicional que se preste, lo que se estima suficiente para cubrir los riesgos derivados del servicio, tiene en cuenta la diversidad de servicios en el mercado y no penaliza a los prestadores con mayor oferta.

Una de las exigencias del Reglamento (UE) 910/2014 se centra en garantizar la seguridad de los servicios de confianza frente a actos deliberados o fortuitos que afecten a sus productos, redes o sistemas de información. En este sentido, todos los prestadores de servicios de confianza, cualificados y no cualificados, están sometidos a la obligación de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que prestan, así como de notificar al órgano de supervisión cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado. Esta Ley sanciona el incumplimiento de las citadas obligaciones.

En respuesta a la evolución de la tecnología y las demandas del mercado, el Reglamento (UE) 910/2014 abre la posibilidad de prestación de servicios innovadores basados en soluciones móviles y en la nube, como la firma y sello electrónicos remotos, en los que el entorno es gestionado por un prestador de servicios de confianza en nombre del titular. A fin de garantizar que estos servicios electrónicos obtengan el mismo reconocimiento jurídico que aquellos utilizados en un entorno completamente gestionado por el usuario, estos prestadores deben aplicar procedimientos de seguridad específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, para garantizar que el entorno es fiable y se utiliza bajo el control exclusivo del titular. Se pretende alcanzar, así, un equilibrio entre la facilidad para el acceso y el uso de los servicios, sin detrimento de la seguridad.

IV

Esta Ley deroga la Ley 59/2003, de 19 de diciembre, de firma electrónica, y con ella aquellos preceptos incompatibles con el Reglamento (UE) 910/2014.

Así sucede con los antiguos certificados de firma de personas jurídicas, introducidos por la citada Ley de firma electrónica. El nuevo paradigma instaurado por el mencionado

reglamento implica que únicamente las personas físicas están capacitadas para firmar electrónicamente, por lo que no prevé la emisión de certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica. A estas se reservan los sellos electrónicos, que permiten garantizar la autenticidad e integridad de documentos tales como facturas electrónicas. Sin perjuicio de lo anterior, las personas jurídicas podrán actuar por medio de los certificados de firma de aquellas personas físicas que legalmente les representen.

La Ley permite la posibilidad de que el órgano supervisor mantenga un servicio de difusión de información sobre los prestadores cualificados que operan en el mercado, con el fin de proporcionar a los usuarios información útil sobre los servicios que ofrecen en el desarrollo de su actividad.

Mediante la presente Ley se deroga también el artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, referido a los terceros de confianza, debido a que los servicios ofrecidos por este tipo de proveedores se encuentran subsumidos en los tipos regulados por el Reglamento (UE) 910/2014, fundamentalmente en los servicios de entrega electrónica certificada y de conservación de firmas y sellos electrónicos.

V

Si bien la prestación de servicios electrónicos de confianza se realiza en régimen de libre competencia, el Reglamento (UE) 910/2014 prevé, para los servicios cualificados, un sistema de verificación previa de cumplimiento de los requisitos que en él se imponen. Así, se diseña un sistema mixto de colaboración público-privada para la supervisión de los prestadores cualificados, pues su inclusión en la lista de confianza, que permite iniciar esa actividad, debe basarse en un informe de evaluación de la conformidad emitido por un organismo de evaluación acreditado por un organismo nacional de acreditación, establecido en alguno de los Estados miembros de la Unión Europea. A partir de entonces, los prestadores cualificados deberán remitir el citado informe al menos cada veinticuatro meses.

Por su parte, los prestadores de servicios no cualificados pueden prestar servicios sin verificación previa de cumplimiento de requisitos, sin perjuicio de su sujeción a las potestades de seguimiento y control posterior de la Administración. No obstante, deberán comunicar al órgano supervisor la prestación del servicio en el plazo de tres meses desde que inicien su actividad, a los meros efectos de conocer su existencia y posibilitar su supervisión.

Por último, se define el régimen sancionador aplicable a los prestadores cualificados y no cualificados de servicios electrónicos de confianza, sin perjuicio de la posibilidad ya prevista en el artículo 20.3 del Reglamento (UE) 910/2014 de retirar la cualificación al prestador o servicio que presta, y su exclusión de la lista de confianza, en determinados supuestos. Asimismo, se han adecuado las cuantías de las sanciones, reduciéndose a la mitad la máxima imponible respecto a la legislación anterior, y se ha previsto la división en tramos de la horquilla sancionadora para la determinación de la multa imponible, en atención a los criterios de graduación concurrentes.

VI

Con arreglo a todo lo anterior, la presente Ley contiene veinte artículos, cuatro disposiciones adicionales, dos transitorias, una disposición derogatoria y siete disposiciones finales.

Las disposiciones adicionales se refieren: la primera a Fe pública y servicios electrónicos de confianza; la segunda a los efectos jurídicos de los sistemas utilizados en las Administraciones públicas; la tercera al Documento Nacional de Identidad y sus certificados electrónicos, y la cuarta al secreto de la identidad de los miembros del Centro Nacional de Inteligencia.

La disposición transitoria primera se refiere a la comunicación de actividad por prestadores de servicios no cualificados ya existentes, y la disposición transitoria segunda mantiene en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, el

cual constituye desarrollo reglamentario parcial de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En las disposiciones finales se modifican diversas leyes. En la primera, la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información, de forma que las empresas que presten servicios al público en general de especial trascendencia económica deberán disponer de un medio seguro de interlocución telemática, no necesariamente basado en certificados electrónicos. Con ello, se flexibiliza la norma y se da cabida a otros medios de identificación generalmente usados en el sector privado.

En la disposición final segunda, se modifica la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, con objeto de adaptarla al nuevo marco regulatorio de los servicios electrónicos de confianza definido en esta Ley y en el Reglamento (UE) 910/2014.

En la disposición final tercera, se modifica la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, para adaptar su regulación al Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, referente a plataformas digitales.

En la disposición final cuarta se introduce una nueva disposición adicional séptima en la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio, para adaptar su regulación al Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimientos de los clientes en el mercado interior.

La disposición final quinta contiene el título competencial, en virtud del cual la Ley se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, telecomunicaciones y seguridad pública, conforme al artículo 149.1.8.ª, 21.ª y 29.ª de la Constitución Española. El artículo 3 y la disposición final segunda se dictan, además, al amparo de lo previsto en el artículo 149.1.6.ª de la Constitución, el cual atribuye al Estado competencia exclusiva en materia de legislación procesal. Por su parte la disposición adicional segunda se dicta al amparo de lo previsto en el artículo 149.1.18.ª de la Constitución, en relación con la competencia estatal exclusiva sobre las bases del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.

Finalmente las disposiciones finales sexta y séptima se refieren al desarrollo reglamentario de la Ley y a su entrada en vigor, respectivamente.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

La presente Ley tiene por objeto regular determinados aspectos de los servicios electrónicos de confianza, como complemento del Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Artículo 2. *Ámbito de aplicación.*

Esta Ley se aplicará a los prestadores públicos y privados de servicios electrónicos de confianza establecidos en España.

Así mismo, se aplicará a los prestadores residentes o domiciliados en otro Estado que tengan un establecimiento permanente situado en España, siempre que ofrezcan servicios no supervisados por la autoridad competente de otro país de la Unión Europea.

Artículo 3. *Efectos jurídicos de los documentos electrónicos.*

1. Los documentos electrónicos públicos, administrativos y privados, tienen el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

2. La prueba de los documentos electrónicos privados en los que se hubiese utilizado un servicio de confianza no cualificado se regirá por lo dispuesto en el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil. Si el servicio fuese cualificado, se estará a lo previsto en el apartado 4 del mismo precepto.

TÍTULO II

Certificados electrónicos

Artículo 4. *Vigencia y caducidad de los certificados electrónicos.*

1. Los certificados electrónicos se extinguen por caducidad a la expiración de su período de vigencia, o mediante revocación por los prestadores de servicios electrónicos de confianza en los supuestos previstos en el artículo siguiente.

2. El período de vigencia de los certificados cualificados no será superior a cinco años.

Dicho período se fijará en atención a las características y tecnología empleada para generar los datos de creación de firma, sello, o autenticación de sitio web.

Artículo 5. *Revocación y suspensión de los certificados electrónicos.*

1. Los prestadores de servicios electrónicos de confianza extinguirán la vigencia de los certificados electrónicos mediante revocación en los siguientes supuestos:

a) Solicitud formulada por el firmante, la persona física o jurídica representada por este, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web.

b) Violación o puesta en peligro del secreto de los datos de creación de firma o de sello, o del prestador de servicios de confianza, o de autenticación de sitio web, o utilización indebida de dichos datos por un tercero.

c) Resolución judicial o administrativa que lo ordene.

d) Fallecimiento del firmante; capacidad modificada judicialmente sobrevenida, total o parcial, del firmante; extinción de la personalidad jurídica o disolución del creador del sello en el caso de tratarse de una entidad sin personalidad jurídica, y cambio o pérdida de control sobre el nombre de dominio en el supuesto de un certificado de autenticación de sitio web.

e) Terminación de la representación en los certificados electrónicos con atributo de representante. En este caso, tanto el representante como la persona o entidad representada están obligados a solicitar la revocación de la vigencia del certificado en cuanto se produzca la modificación o extinción de la citada relación de representación.

f) Cese en la actividad del prestador de servicios de confianza salvo que la gestión de los certificados electrónicos expedidos por aquel sea transferida a otro prestador de servicios de confianza.

g) Descubrimiento de la falsedad o inexactitud de los datos aportados para la expedición del certificado y que consten en él, o alteración posterior de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo.

h) En caso de que se advierta que los mecanismos criptográficos utilizados para la generación de los certificados no cumplen los estándares de seguridad mínimos necesarios para garantizar su seguridad.

i) Cualquier otra causa lícita prevista en la declaración de prácticas del servicio de confianza.

2. Los prestadores de servicios de confianza suspenderán la vigencia de los certificados electrónicos en los supuestos previstos en las letras a), c) y h) del apartado anterior, así como en los casos de duda sobre la concurrencia de las circunstancias previstas en sus letras b) y g), siempre que sus declaraciones de prácticas de certificación prevean la posibilidad de suspender los certificados.

3. En su caso, y de manera previa o simultánea a la indicación de la revocación o suspensión de un certificado electrónico en el servicio de consulta sobre el estado de validez o revocación de los certificados por él expedidos, el prestador de servicios electrónicos de confianza comunicará al titular, por un medio que acredite la entrega y recepción efectiva

siempre que sea factible, esta circunstancia, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

En los casos de suspensión, la vigencia del certificado se extinguirá si transcurrido el plazo de duración de la suspensión, el prestador no la hubiera levantado.

Artículo 6. *Identidad y atributos de los titulares de certificados cualificados.*

1. La identidad del titular en los certificados cualificados se consignará de la siguiente forma:

a) En el supuesto de certificados de firma electrónica y de autenticación de sitio web expedidos a personas físicas, por su nombre y apellidos y su número de Documento Nacional de Identidad, número de identidad de extranjero o número de identificación fiscal, o a través de un pseudónimo que conste como tal de manera inequívoca. Los números anteriores podrán sustituirse por otro código o número identificativo únicamente en caso de que el titular carezca de todos ellos por causa lícita, siempre que le identifique de forma unívoca y permanente en el tiempo.

b) En el supuesto de certificados de sello electrónico y de autenticación de sitio web expedidos a personas jurídicas, por su denominación o razón social y su número de identificación fiscal. En defecto de este, deberá indicarse otro código identificativo que le identifique de forma unívoca y permanente en el tiempo, tal como se recoja en los registros oficiales.

2. Si los certificados admiten una relación de representación incluirán la identidad de la persona física o jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento, público si resulta exigible, que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales.

Artículo 7. *Comprobación de la identidad y otras circunstancias de los solicitantes de un certificado cualificado.*

1. La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el Documento Nacional de Identidad, pasaporte u otros medios admitidos en Derecho. Podrá prescindirse de la personación de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

2. Reglamentariamente, mediante Orden de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, se determinarán otras condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física según su evaluación por un organismo de evaluación de la conformidad. La determinación de dichas condiciones y requisitos técnicos se realizará a partir de los estándares que, en su caso, hayan sido determinados a nivel comunitario.

Serán considerados métodos de identificación reconocidos a escala nacional, a los efectos de lo previsto en el presente apartado, aquellos que aporten una seguridad equivalente en términos de fiabilidad a la presencia física y cuya equivalencia en el nivel de seguridad sea certificada por un organismo de evaluación de la conformidad, de acuerdo con lo previsto en la normativa en materia de servicios electrónicos de confianza.

3. La forma en que se ha procedido a identificar a la persona física solicitante podrá constar en el certificado. En otro caso, los prestadores de servicios de confianza deberán colaborar entre sí para determinar cuándo se produjo la última personación.

4. En el caso de certificados cualificados de sello electrónico y de firma electrónica con atributo de representante, los prestadores de servicios de confianza comprobarán, además de los datos señalados en los apartados anteriores, los datos relativos a la constitución y personalidad jurídica, y a la persona o entidad representada, respectivamente, así como la extensión y vigencia de las facultades de representación del solicitante mediante los documentos, públicos si resultan exigibles, que sirvan para acreditar los extremos citados de

manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. Esta comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

5. Cuando el certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, estas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

6. Lo dispuesto en los apartados anteriores podrá no ser exigible cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de confianza en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubiese empleado el medio señalado en el apartado 1 y el período de tiempo transcurrido desde la identificación fuese menor de cinco años.

7. El Ministerio de Asuntos Económicos y Transformación Digital velará por que los prestadores cualificados de servicios electrónicos de confianza puedan contribuir a la elaboración de la norma reglamentaria prevista en el apartado 2 del presente artículo, de acuerdo con lo previsto en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

TÍTULO III

Obligaciones y responsabilidad de los prestadores de servicios electrónicos de confianza

Artículo 8. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios electrónicos de confianza para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta Ley se sujetará a lo dispuesto en la legislación aplicable en materia de protección de datos de carácter personal.

2. Los prestadores de servicios electrónicos de confianza que consignen un pseudónimo en un certificado electrónico deberán constatar la verdadera identidad del titular del certificado y conservar la documentación que la acredite.

3. Dichos prestadores de servicios de confianza estarán obligados a revelar la citada identidad cuando lo soliciten los órganos judiciales y otras autoridades públicas en el ejercicio de funciones legalmente atribuidas, con sujeción a lo dispuesto en la legislación aplicable en materia de protección de datos personales.

Artículo 9. *Obligaciones de los prestadores de servicios electrónicos de confianza.*

1. Los prestadores de servicios electrónicos de confianza deberán:

a) Publicar información veraz y acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

En este caso, utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deberán custodiar y proteger los datos de creación de firma, sello o autenticación de sitio web frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad.

2. Los prestadores de servicios de confianza que expidan certificados electrónicos deberán disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados emitidos accesible al público.

3. Los prestadores cualificados de servicios electrónicos de confianza deberán cumplir las siguientes obligaciones adicionales:

a) El período de tiempo durante el que deberán conservar la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014, será de 15 años desde la extinción del certificado o la finalización del servicio prestado.

En caso de que expidan certificados cualificados de sello electrónico o autenticación de sitio web a personas jurídicas, los prestadores de servicios de confianza registrarán también la información que permita determinar la identidad de la persona física a la que se hayan entregado los citados certificados, para su identificación en procedimientos judiciales o administrativos.

b) Constituir un seguro de responsabilidad civil por importe mínimo de 1.500.000 euros, excepto si el prestador pertenece al sector público. Si presta más de un servicio cualificado de los previstos en el Reglamento (UE) 910/2014, se añadirán 500.000 euros más por cada tipo de servicio.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo dispuesto en el párrafo anterior.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto.

c) El prestador cualificado que vaya a cesar en su actividad deberá comunicarlo a los clientes a los que preste sus servicios y al órgano de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad, por un medio que acredite la entrega y recepción efectiva siempre que sea factible. El plan de cese del prestador de servicios puede incluir la transferencia de clientes, una vez acreditada la ausencia de oposición de los mismos, a otro prestador cualificado, el cual podrá conservar la información relativa a los servicios prestados hasta entonces.

Igualmente, comunicará al órgano de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

d) Enviar el informe de evaluación de la conformidad al Ministerio de Asuntos Económicos y Transformación Digital en los términos previstos en el artículo 20.1 del Reglamento (UE) 910/2014. El incumplimiento de esta obligación conllevará la retirada de la cualificación al prestador y al servicio que este presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento, previo requerimiento al prestador del servicio para que cese en el citado incumplimiento.

Artículo 10. *Responsabilidad de los prestadores de servicios electrónicos de confianza.*

Los prestadores de servicios electrónicos de confianza asumirán toda la responsabilidad frente a terceros por la actuación de las personas u otros prestadores en los que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios electrónicos de confianza, incluyendo las actuaciones de comprobación de identidad previas a la expedición de un certificado cualificado.

Artículo 11. *Limitaciones de responsabilidad de los prestadores de servicios electrónicos de confianza.*

1. El prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe, si esta incurre en alguno de los supuestos previstos en el Reglamento (UE) 910/2014 o en los siguientes:

a) No haber proporcionado al prestador de servicios de confianza información veraz, completa y exacta para la prestación del servicio de confianza, en particular, sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada, actuando con la debida diligencia, por el prestador de servicios.

b) La falta de comunicación sin demora indebida al prestador de servicios de cualquier modificación de las circunstancias que incidan en la prestación del servicio de confianza, en particular, aquellas reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, sello o autenticación de sitio web, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos.

d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma, sello o autenticación de sitio web o, en su caso, de los medios que den acceso a ellos.

e) Utilizar los datos de creación de firma, sello o autenticación de sitio web cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de confianza le notifique la extinción o suspensión de su vigencia.

2. El prestador de servicios de confianza tampoco será responsable por los daños y perjuicios si el destinatario actúa de forma negligente. Se entenderá que el destinatario actúa de forma negligente cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico, o cuando no verifique la firma o sello electrónico.

3. El prestador de servicios de confianza no será responsable por los daños y perjuicios en caso de inexactitud de los datos que consten en el certificado electrónico si estos le han sido acreditados mediante documento público u oficial, inscrito en un registro público si así resulta exigible.

Artículo 12. *Inicio de la prestación de servicios electrónicos de confianza no cualificados.*

Los prestadores de servicios de confianza no cualificados no necesitan verificación administrativa previa de cumplimiento de requisitos para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses desde que la inicien, que publicará en su página web el listado de prestadores de servicios de confianza no cualificados en una lista diferente a la de los prestadores de servicios de confianza cualificados, con la descripción detallada y clara de las características propias y diferenciales de los prestadores cualificados y de los prestadores no cualificados.

En el mismo plazo deberán comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad.

Artículo 13. *Obligaciones de seguridad de la información.*

1. Los prestadores cualificados y no cualificados de servicios electrónicos de confianza notificarán al Ministerio de Asuntos Económicos y Transformación Digital las violaciones de seguridad o pérdidas de la integridad señaladas en el artículo 19.2 del Reglamento (UE) 910/2014, sin perjuicio de su notificación a la Agencia Española de Protección de Datos, a otros organismos relevantes o a las personas afectadas.

2. Los prestadores de servicios tienen la obligación de tomar las medidas necesarias para resolver los incidentes de seguridad que les afecten.

3. Los prestadores de servicios ampliarán, en un plazo máximo de un mes tras la notificación del incidente y, de haber tenido lugar, tras su resolución, la información suministrada en la notificación inicial con arreglo a las directrices y formularios que pueda establecer el Ministerio de Asuntos Económicos y Transformación Digital.

TÍTULO IV

Supervisión y control

Artículo 14. *Órgano de supervisión.*

1. El Ministerio de Asuntos Económicos y Transformación Digital, como órgano de supervisión, controlará el cumplimiento por los prestadores de servicios electrónicos de confianza cualificados y no cualificados que ofrezcan sus servicios al público de las obligaciones establecidas en el Reglamento (UE) 910/2014 y en esta Ley.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá acordar las medidas apropiadas para el cumplimiento del Reglamento (UE) 910/2014 y de esta Ley.

En particular, podrá dictar directrices para la elaboración y comunicación de informes y documentos, así como recomendaciones para el cumplimiento de las obligaciones técnicas y de seguridad exigibles a los servicios de confianza, así como sobre requisitos y normas técnicas de auditoría y certificación para la evaluación de la conformidad de los prestadores cualificados de servicios de confianza. Al efecto, se tendrán en consideración las normas, instrucciones, guías y recomendaciones emitidas por el Centro Criptológico Nacional en el marco de sus competencias, así como informes, especificaciones o normas elaboradas por la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) o por organismos de estandarización europeos e internacionales.

Artículo 15. *Actuaciones inspectoras.*

1. El Ministerio de Asuntos Económicos y Transformación Digital realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de supervisión y control. Los funcionarios adscritos al Ministerio de Asuntos Económicos y Transformación Digital que realicen la inspección tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

2. El Ministerio de Asuntos Económicos y Transformación Digital podrá recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de confianza que le asigna el Reglamento (UE) 910/2014 y esta Ley.

3. Podrá requerirse la realización de pruebas en laboratorios o entidades especializadas para acreditar el cumplimiento de determinados requisitos. En este caso, los prestadores de servicios correrán con los gastos que ocasione esta evaluación.

Artículo 16. *Mantenimiento de la lista de confianza.*

1. El Ministerio de Asuntos Económicos y Transformación Digital establecerá, mantendrá y publicará la lista de confianza con información relativa a los prestadores cualificados de servicios de confianza sujetos a esta Ley, junto con la información relacionada con los servicios de confianza cualificados prestados por ellos, según lo previsto en el artículo 22 del Reglamento (UE) 910/2014.

2. El plazo máximo para dictar y notificar resolución en el procedimiento de verificación previa de cumplimiento de los requisitos establecidos en el citado Reglamento será de 6 meses, transcurridos los cuales se podrá entender desestimada la solicitud.

3. La revocación de la cualificación a un prestador o a un servicio mediante su retirada de la lista de confianza es independiente de la aplicación del régimen sancionador.

Artículo 17. *Información y colaboración.*

1. Los prestadores de servicios de confianza, la entidad nacional de acreditación, los organismos de evaluación de la conformidad, los organismos de certificación y cualquier otra persona o entidad relacionada con el prestador de servicios de confianza, tienen la obligación de facilitar al Ministerio de Asuntos Económicos y Transformación Digital toda la información y colaboración precisas para el ejercicio de sus funciones.

Si el organismo de certificación perteneciera a la Autoridad Nacional de Certificación de la Ciberseguridad o estuviese supervisado por ella, se acordarán con dicha Autoridad los mecanismos de colaboración y el contenido de la información necesaria.

Los prestadores de servicios de confianza deberán permitir a sus funcionarios o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquellas.

2. La información referente a los prestadores cualificados de servicios de confianza podrá ser objeto de publicación en la dirección de Internet del Ministerio de Asuntos Económicos y Transformación Digital para su difusión y conocimiento.

3. A más tardar el 1 de febrero de cada año, los prestadores cualificados de servicios de confianza remitirán al Ministerio de Asuntos Económicos y Transformación Digital un informe

sobre sus datos de actividad del año civil precedente, con objeto de cumplimiento por parte de este de las obligaciones de información a la Comisión Europea.

4. El Ministerio de Asuntos Económicos y Transformación Digital informará a la Agencia Española de Protección de Datos en caso de resultar infringidas las normas sobre protección de datos de carácter personal, así como sobre los incidentes en materia de seguridad que impliquen violaciones de los datos de carácter personal.

TÍTULO V

Infracciones y sanciones

Artículo 18. *Infracciones.*

1. Las infracciones de los preceptos del Reglamento (UE) 910/2014 y de esta Ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) La comisión de una infracción grave en el plazo de dos años desde que hubiese sido sancionado por una infracción grave de la misma naturaleza, contados desde que recaiga la resolución sancionadora firme.

b) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando ello afecte a la mayoría de los certificados cualificados expedidos en el año anterior al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este periodo es menor.

3. Son infracciones graves:

a) La resistencia, obstrucción, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley.

b) Actuar en el mercado como prestador cualificado de servicios de confianza, ofrecer servicios de confianza como cualificados o utilizar la etiqueta de confianza «UE» sin haber obtenido la cualificación de los citados servicios.

c) En caso de que el prestador expida certificados electrónicos, almacenar o copiar, por sí o a través de un tercero, los datos de creación de firma, sello o autenticación de sitio web de la persona física o jurídica a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del titular.

d) No proteger adecuadamente los datos de creación de firma, sello o autenticación de sitio web cuya gestión se le haya encomendado en la forma establecida en el artículo 9.1.b) de esta Ley.

e) No registrar o conservar la información a la que se refiere el artículo 9.3.a) de esta Ley.

f) El incumplimiento de la obligación de notificación de incidentes establecida en el artículo 19.2 del Reglamento (UE) 910/2014, en los términos previstos en el artículo 13 de esta Ley.

g) En caso de prestadores cualificados de servicios de confianza, el incumplimiento de alguna de las obligaciones establecidas en los artículos 24.2, letras b), c), d), e), f), g), h), y k), 24.3 y 24.4 del Reglamento (UE) 910/2014, con las precisiones establecidas, en su caso, por esta Ley.

h) La expedición de certificados cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado o al poder de representación de quien lo solicita en su nombre, señaladas en el Reglamento (UE) 910/2014 y en esta Ley, cuando no constituya infracción muy grave.

i) La ausencia de adopción de medidas, o la adopción de medidas insuficientes, para la resolución de los incidentes de seguridad en los productos, redes y sistemas de información, en el plazo de diez días desde que aquellos se hubieren producido.

j) El incumplimiento de las resoluciones dictadas por el Ministerio de Asuntos Económicos y Transformación Digital para requerir a un prestador de servicios de confianza

que corrija cualquier incumplimiento de los requisitos establecidos en esta Ley y en el Reglamento (UE) 910/2014.

k) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control, a partir del segundo requerimiento.

l) No cumplir con las obligaciones de constatar la verdadera identidad del titular de un certificado electrónico y de conservar la documentación que la acredite, en caso de consignación de un pseudónimo.

m) El incumplimiento por parte de los prestadores cualificados y no cualificados de servicios de confianza de la obligación establecida en el artículo 19.1 del Reglamento (UE) 910/2014 de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los servicios de confianza que presten.

n) No extinguir la vigencia de los certificados electrónicos en los supuestos señalados en esta Ley.

o) La prestación de servicios cualificados careciendo del correspondiente seguro obligatorio, en los términos previstos en el artículo 9.3.b) de esta Ley.

4. Constituyen infracciones leves:

a) Publicar información no veraz o no acorde con esta Ley y el Reglamento (UE) 910/2014.

b) No comunicar el inicio de actividad, su modificación o cese por los prestadores de servicios no cualificados en el plazo establecido en el artículo 12 de esta Ley.

c) El incumplimiento por los prestadores cualificados de servicios de confianza de alguna de las obligaciones establecidas en el artículo 24.2, letras a) e i) del Reglamento (UE) 910/2014.

d) El incumplimiento por los prestadores cualificados de servicios de confianza de su obligación de remitir un informe anual de actividad al Ministerio de Asuntos Económicos y Transformación Digital antes del 1 de febrero de cada año.

e) El incumplimiento del deber de comunicación establecido en el artículo 9.3.c) de esta Ley.

f) La falta o deficiente presentación de información solicitada por parte del Ministerio de Asuntos Económicos y Transformación Digital en su función de inspección y control.

Artículo 19. *Sanciones.*

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán al infractor las siguientes sanciones:

a) Por la comisión de infracciones muy graves, una multa por importe de 150.001 hasta 300.000 euros.

b) Por la comisión de infracciones graves, una multa por importe de 50.001 hasta 150.000 euros.

c) Por la comisión de infracciones leves, una multa por importe de hasta 50.000 euros.

2. La cuantía de las sanciones que se impongan se determinará aplicando una graduación de importe mínimo, medio y máximo a cada nivel de infracción, teniendo en cuenta lo siguiente:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza y cuantía de los perjuicios causados.

d) La reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme en vía administrativa.

e) El volumen de facturación del prestador responsable.

f) El número de personas afectadas por la infracción.

g) La gravedad del riesgo generado por la conducta.

h) Las acciones realizadas por el prestador encaminadas a paliar los efectos o consecuencias de la infracción.

3. Las resoluciones sancionadoras por la comisión de infracciones muy graves serán publicadas en el sitio de Internet del Ministerio de Asuntos Económicos y Transformación Digital, con indicación, en su caso, de los recursos interpuestos contra ellas.

Artículo 19 bis. *Apercibimiento.*

1. Los órganos con competencia sancionadora, atendida la naturaleza de los hechos y la concurrencia significativa de los criterios establecidos en el artículo anterior, podrán acordar no iniciar la apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable, a fin de que en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que, en cada caso, resulten pertinentes, siempre que los hechos fuesen constitutivos de infracción leve o grave conforme a lo dispuesto en esta ley.

2. Si el apercibimiento no fuera atendido en el plazo que el órgano sancionador hubiera determinado, procederá la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

Artículo 20. *Potestad sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.

Disposición adicional primera. *Fe pública y servicios electrónicos de confianza.*

Lo dispuesto en esta Ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente atribuida la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias.

Disposición adicional segunda. *Efectos jurídicos de los sistemas utilizados en las Administraciones públicas.*

Todos los sistemas de identificación, firma y sello electrónico previstos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, tendrán plenos efectos jurídicos.

Disposición adicional tercera. *Documento Nacional de Identidad y sus certificados electrónicos.*

1. El Documento Nacional de Identidad electrónico es el Documento Nacional de Identidad que permite acreditar electrónicamente la identidad personal de su titular, en los términos establecidos en el artículo 8 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana, así como la firma electrónica de documentos.

2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del Documento Nacional de Identidad para acreditar la identidad y los demás datos personales del titular que consten en el mismo, así como la identidad del firmante y la integridad de los documentos firmados con sus certificados electrónicos.

3. Los órganos competentes del Ministerio del Interior para la expedición del Documento Nacional de Identidad cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios electrónicos de confianza que expidan certificados cualificados.

4. Sin perjuicio de la aplicación de la normativa vigente en materia del Documento Nacional de Identidad en todo aquello que se adecúe a sus características particulares, el Documento Nacional de Identidad se regirá por su normativa específica.

Disposición adicional cuarta. *Secreto de la identidad de los miembros del Centro Nacional de Inteligencia.*

Lo dispuesto en los artículos 7 y 8 de esta Ley se entenderá sin perjuicio de lo dispuesto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, en relación con la obligación de guardar secreto sobre la identidad de sus miembros.

Disposición transitoria primera. *Comunicación de actividad por prestadores de servicios no cualificados ya existentes.*

Los prestadores de servicios no cualificados que ya vinieran prestando servicios deberán comunicar su actividad al Ministerio de Asuntos Económicos y Transformación Digital en el plazo de tres meses a contar desde la entrada en vigor de esta Ley.

Se exceptúan aquellos que hubieran comunicado los servicios prestados al Ministerio de Asuntos Económicos y Transformación Digital antes de la entrada en vigor de esta Ley.

Disposición transitoria segunda. *Desarrollo reglamentario del Documento Nacional de Identidad.*

Hasta que se desarrolle reglamentariamente el Documento Nacional de Identidad, se mantendrá en vigor el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

Disposición derogatoria.

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley, y en particular:

a) La Ley 59/2003, de 19 de diciembre, de firma electrónica.

b) El artículo 25 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

c) La Orden del Ministerio de Fomento de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

Disposición final primera. *Modificación de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.*

Se modifica el apartado 1 del artículo 2 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, que queda redactado como sigue:

> «1. Sin perjuicio de la utilización de otros medios de comunicación a distancia con los clientes, las empresas que presten servicios al público en general de especial trascendencia económica deberán facilitar a sus usuarios un medio seguro de interlocución telemática que les permita la realización de, al menos, los siguientes trámites:
>
> a) Contratación electrónica de servicios, suministros y bienes, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico entre las partes, sin perjuicio de lo establecido en la normativa sectorial.
>
> b) Consulta de sus datos de cliente, que incluirán información sobre su historial de facturación de, al menos, los últimos tres años y el contrato suscrito, incluidas las condiciones generales si las hubiere.
>
> c) Presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, garantizando la constancia de su presentación para el consumidor y asegurando una atención personal directa.
>
> d) Ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.»

Disposición final segunda. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Uno. Se modifica el apartado 3 del artículo 326 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado en los siguientes términos:

«3. Cuando la parte a quien interese la eficacia de un documento electrónico lo solicite o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico que un servicio electrónico de confianza no cualificado de los previstos en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, permita acreditar, se procederá con arreglo a lo establecido en el apartado 2 del presente artículo y en el Reglamento (UE) n.º 910/2014.»

Dos. Se añade un apartado 4 al citado artículo 326, con el siguiente tenor:

«4. Si se hubiera utilizado algún servicio de confianza cualificado de los previstos en el Reglamento citado en el apartado anterior, se presumirá que el documento reúne la característica cuestionada y que el servicio de confianza se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza de prestadores y servicios cualificados.

Si aun así se impugnare el documento electrónico, la carga de realizar la comprobación corresponderá a quien haya presentado la impugnación. Si dichas comprobaciones obtienen un resultado negativo, serán las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación. Si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 300 a 1200 euros.»

Disposición final tercera. *Modificación de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.*

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se modifica en los siguientes términos:

Uno. Se añade un nuevo artículo 12 ter que queda redactado como sigue:

«Artículo 12 ter. *Obligaciones relativas a la portabilidad de datos no personales.*

Los proveedores de servicios de intermediación que alojen o almacenen datos de usuarios a los que presten servicios de redes sociales o servicios de la sociedad de la información equivalentes deberán remitir a dichos usuarios, a su solicitud, los contenidos que les hubieran facilitado, sin impedir su transmisión posterior a otro proveedor. La remisión deberá efectuarse en un formato estructurado, de uso común y lectura mecánica.

Asimismo, deberán transmitir dichos contenidos directamente a otro proveedor designado por el usuario, siempre que sea técnicamente posible, según prevé el artículo 95 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Para el cumplimiento de estas obligaciones será aplicable lo dispuesto en el artículo 12.5 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.»

Dos. El primer párrafo del apartado 1 del artículo 35 queda redactado como sigue:

«1. El Ministerio de Asuntos Económicos y Transformación Digital controlará el cumplimiento por los prestadores de servicios de la sociedad de la información de las obligaciones establecidas en esta Ley y en sus disposiciones de desarrollo, en lo que se refiere a los servicios propios de la sociedad de la información, así como en el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de

2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, por parte de aquellos proveedores incluidos en su ámbito de aplicación.»

Tres. Se añade un nuevo artículo 36 bis que queda redactado como sigue:

«Artículo 36 bis. *Deber de comunicación de las organizaciones y asociaciones representativas de usuarios profesionales o de los usuarios de sitios web corporativos.*

Las organizaciones y asociaciones que posean un interés legítimo de representación de usuarios profesionales o de los usuarios de sitios web corporativos, y que, cumpliendo con los requisitos del artículo 14.3 del Reglamento (UE) 2019/1150, hubieren solicitado al Ministerio de Asuntos Económicos y Transformación Digital su inclusión en la lista elaborada al efecto por la Comisión Europea, notificarán inmediatamente al citado Ministerio cualquier circunstancia que afecte a su entidad que derive en un incumplimiento sobrevenido de los mencionados requisitos.»

Cuatro. El primer párrafo del artículo 37 queda redactado como sigue:

«Los prestadores de servicios de la sociedad de la información a los que les sea de aplicación la presente Ley, así como los proveedores incluidos en el ámbito de aplicación del Reglamento (UE) 2019/1150, están sujetos al régimen sancionador establecido en este Título.»

Cinco. Se añaden doce nuevas letras de la j) a la u) al apartado 3 del artículo 38 con la siguiente redacción:

«j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, fuera de los supuestos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679.

k) El incumplimiento habitual de la obligación prevista en el artículo 12 ter.

l) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional.

m) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150.

n) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables.

o) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos.

p) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea o los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios.

q) El incumplimiento por parte de los proveedores de servicios de intermediación de la obligación establecida en la letra a) del artículo 8 del Reglamento (UE) 2019/1150, así como el incumplimiento habitual de las obligaciones contenidas en las letras b) y c) del citado precepto.

r) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150.

s) El incumplimiento habitual por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150.

t) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de establecer un sistema interno y gratuito para tramitar las reclamaciones de los usuarios profesionales, en los términos previstos por el artículo 11 del Reglamento (UE) 2019/1150.

u) El incumplimiento por parte de los proveedores de servicios de intermediación en línea que no sean pequeñas empresas, de la obligación de designar al menos dos mediadores, o de cualquier otra de las obligaciones en materia de mediación establecidas en el artículo 12 del Reglamento (UE) 2019/1150.»

Seis. Se añaden diez nuevas letras de la j) a la s) al apartado 4 del artículo 38 con la siguiente redacción:

«j) La exigencia del pago de un canon por atender la obligación prevista en el artículo 12 ter, cuando así lo permita el artículo 12.5 del Reglamento (UE) 2016/679, si su cuantía excediese el importe de los costes afrontados.

k) El incumplimiento de la obligación prevista en el artículo 12 ter, cuando no constituya infracción grave.

l) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación establecida en el apartado 5 del artículo 3 del Reglamento (UE) 2019/1150 en materia de visibilidad de la identidad del usuario profesional, cuando no constituya infracción grave.

m) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de cualquiera de las obligaciones en materia de restricción, suspensión y terminación del servicio establecidas en los apartados 1, 2 y 3 del artículo 4 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

n) El incumplimiento por parte de los proveedores de servicios de intermediación en línea o proveedores de motores de búsqueda en línea de cualquiera de las obligaciones en materia de clasificación establecidas en el artículo 5 del Reglamento (UE) 2019/1150 que les resulten aplicables, cuando no constituya infracción grave.

o) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de incluir en sus condiciones generales la información exigida en el artículo 6 del Reglamento (UE) 2019/1150 sobre los bienes y servicios auxiliares ofrecidos, cuando no constituya infracción grave.

p) El incumplimiento por parte de los proveedores de servicios de intermediación en línea y los proveedores de motores de búsqueda en línea de la obligación de incluir en sus condiciones generales la información exigida en los apartados 1 y 2, respectivamente, con las precisiones establecidas en el apartado 3, del artículo 7 del Reglamento (UE) 2019/1150, en materia de tratamiento diferenciado de bienes o servicios, cuando no constituya infracción grave.

q) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de las obligaciones en materia de cláusulas contractuales específicas establecidas en el artículo 8 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

r) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de informar sobre el acceso a datos por parte de los usuarios profesionales establecida en el artículo 9 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.

s) El incumplimiento por parte de los proveedores de servicios de intermediación en línea de la obligación de justificar las restricciones a la oferta de condiciones diferentes por otros medios prevista en el artículo 10 del Reglamento (UE) 2019/1150, cuando no constituya infracción grave.»

Siete. El artículo 43 queda redactado como sigue:

«Artículo 43. *Competencia sancionadora.*

1. La imposición de sanciones por el incumplimiento de lo previsto en esta Ley corresponderá, en el caso de infracciones muy graves, a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital, y en el de infracciones graves y leves, a la persona titular de la Secretaria de Estado de Digitalización e Inteligencia Artificial.

No obstante lo anterior, la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refieren las letras a) y b) del artículo 38.2 de esta Ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta Ley.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y en sus normas de desarrollo. El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de iniciación. El plazo máximo de duración del procedimiento simplificado será de tres meses.»

Disposición final cuarta. *Modificación de la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.*

Se introduce una nueva disposición adicional séptima con el siguiente contenido:

«Disposición adicional séptima. *Incumplimiento de la prohibición de discriminación.*

El incumplimiento de la prohibición de discriminación prevista en el artículo 16.3 de esta Ley y el Reglamento (UE) 2018/302 del Parlamento Europeo y del Consejo, de 28 de febrero de 2018, sobre medidas destinadas a impedir el bloqueo geográfico injustificado y otras formas de discriminación por razón de la nacionalidad, del lugar de residencia o del lugar de establecimiento de los clientes en el mercado interior y por el que se modifican los Reglamentos (CE) 2006/2004 y (UE) 2017/2394 y la Directiva 2009/22/CE, se reputará desleal a los efectos de la Ley 3/1991, de 10 de enero, de Competencia Desleal, sin perjuicio del régimen de infracciones y sanciones contenido en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.»

Disposición final quinta. *Título competencial.*

Esta Ley se dicta al amparo de las competencias exclusivas que corresponden al Estado en materia de legislación civil, telecomunicaciones y seguridad pública, conforme a lo dispuesto en el artículo 149.1.8.ª, 21.ª y 29.ª de la Constitución Española.

El artículo 3 y la disposición final segunda se dictan, además, al amparo de lo previsto en el artículo 149.1.6.ª de la Constitución, el cual atribuye al Estado competencia exclusiva en materia de legislación procesal. Por su parte la disposición adicional segunda se dicta al amparo de lo previsto en el artículo 149.1.18.ª de la Constitución, en relación con la competencia estatal exclusiva sobre las bases del régimen jurídico de las Administraciones públicas y el procedimiento administrativo común.

Disposición final sexta. *Desarrollo reglamentario.*

Se habilita al Gobierno para dictar las disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta Ley.

Disposición final séptima. *Entrada en vigor.*

La presente Ley entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 12

Resolución de 29 de noviembre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se publica el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados de la Administración General del Estado y se anuncia su publicación en la sede correspondiente

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 299, de 13 de diciembre de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-15066

El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, establece, en su artículo 24, apartado 3, que la política de firma electrónica y de certificados en el ámbito de la Administración General del Estado y de sus organismos públicos será aprobada por el Consejo Superior de Administración Electrónica.

Así mismo, señala que el Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados extractado se publicará en el «Boletín Oficial del Estado», mediante resolución del Secretario de Estado para la Función Pública, y de forma íntegra en la sede del punto de acceso general de la Administración General del Estado.

De conformidad con el Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, las funciones de la Secretaría de Estado para la Función Pública son asumidas por la Secretaría de Estado de Administraciones Públicas.

El Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012, aprobó la Política de Firma Electrónica y de Certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, de conformidad con lo previsto en el artículo 24, apartado 3, del citado Real Decreto 1671/2009.

En su virtud, y en aplicación de lo dispuesto en el mencionado artículo 24, apartado 3, del Real Decreto 1671/2009, esta Secretaría de Estado resuelve:

Primero.

Ordenar la publicación en el «Boletín Oficial del Estado» del Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, adoptado por el Consejo Superior de Administración Electrónica, en reunión de la Comisión Permanente de 30 de mayo de 2012, en cumplimiento de lo previsto en el artículo 24, apartado 3, de Real Decreto 1671/2009, y que se incluye en esta Resolución como anexo.

Segundo.

Ordenar la publicación íntegra en la sede del punto de acceso general de la Administración General del Estado (ver datos de acceso en el siguiente apartado) de los documentos comprensivos de la política de firma electrónica basada en certificados en el ámbito de la Administración General del Estado y de sus organismos públicos y de los perfiles de los certificados electrónicos, constituidos por los anexos I, Política de firma electrónica y de certificados de la Administración General del Estado, y II, Perfiles de certificados electrónicos, en forma de documentos electrónicos en formato PDF firmados electrónicamente el día 19 de noviembre de 2012 por la Presidenta de la Comisión Permanente del Consejo Superior de Administración Electrónica, doña María Ester Arizmendi Gutiérrez, de forma que sus códigos de verificación electrónicos se puedan comprobar en la sede de la Secretaría de Estado de Administraciones Públicas en la dirección provisional https://sede.mpt.gob.es/valida, todo ello sin perjuicio de que puedan ser publicados en otras sedes electrónicas.

Tercero.

Ordenar la publicación extractada en el «Boletín Oficial del Estado» de los datos de acceso y códigos de verificación electrónicos de los documentos comprensivos de la política de firma electrónica basada en certificados en el ámbito de la Administración General del Estado y de sus organismos públicos y de los perfiles de los certificados electrónicos, constituidos por los anexos I, Política de firma electrónica y de certificados de la Administración General del Estado, y II, Perfiles de certificados electrónicos, para que se pueda verificar la integridad de los mismos (se incluyen códigos QR para acceder, desde dispositivos móviles, a los ficheros y a la información de los códigos de verificación respectivos):

Documento: Anexo I, Política de firma electrónica y de certificados de la Administración General del Estado.
Dirección o URL: https://sede.060.gob.es/politica_de_firma_anexo_1.pdf.
Tamaño de fichero: 178.383 bytes.
Código de verificación electrónico: C4075E8D7946EF14B65819F01C2D5F63.

Dirección o URL: CVE:

Documento: Anexo II, Perfiles de certificados electrónicos.
Dirección o URL: https://sede.060.gob.es/perfiles_de_certificados_anexo_2.pdf.
Tamaño de fichero: 363.674 bytes.
Código de verificación electrónico: 483AFA7835C0CF999551DF4992EE945D.

Dirección o URL: CVE:

Cuarto.

La política de firma electrónica y de certificados de la Administración General del Estado, se aplicará en el plazo de un mes siguiente a la publicación de esta Resolución en el «Boletín Oficial del Estado».

ANEXO

Acuerdo de aprobación de la Política de Firma Electrónica y de Certificados en el ámbito de la Administración General del Estado y de sus organismos públicos

Doña Manuela de Paz Prieto, Secretaria de la Comisión Permanente del Consejo Superior de Administración Electrónica,

CERTIFICA, que en la 82.ª reunión de la Comisión Permanente del Consejo Superior de Administración Electrónica, celebrada en Madrid, en la sede del Ministerio de Hacienda y Administraciones Públicas, calle María de Molina, 50, el día treinta de mayo de dos mil doce, en cumplimiento del acuerdo sobre delegación de competencias en la Comisión Permanente, del Pleno del Consejo Superior de Administración Electrónica celebrado el 3 de abril de 2006, se adoptó, entre otros, el siguiente acuerdo:

Informar favorablemente la Resolución de la Secretaría de Estado de Administraciones Públicas, por la que se establece la Política de Firma Electrónica y de Certificados de la Administración General del Estado, en los términos que se recogen en los documentos que se acompañan como anexos, en ejercicio de las funciones atribuidas en el artículo 4.1.c) del Real Decreto 589/2005, de 20 de mayo, por el que se reestructuran los órganos colegiados responsables de la Administración electrónica.

Se hace constar, en aplicación de lo dispuesto en el apartado 5 del artículo 27 de la Ley 30/1992, de 26 de noviembre, que el Acta de la sesión donde se adoptó el presente acuerdo se someterá a la aprobación de la Comisión Permanente en su siguiente reunión.

Y para que conste, se firma el presente certificado en Madrid, a 29 de junio de 2012.

§ 13

Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica

Ministerio del Interior
«BOE» núm. 307, de 24 de diciembre de 2005
Última modificación: 30 de mayo de 2015
Referencia: BOE-A-2005-21163

La Ley Orgánica 1/1992, de 21 de febrero, sobre Protección de la Seguridad Ciudadana, en su artículo 9, reconoce el derecho de todos los españoles a que se les expida el Documento Nacional de Identidad, al que se atribuye el valor suficiente para acreditar, por sí solo, la identidad de las personas y le otorga la protección que a los documentos públicos y oficiales es reconocida por el ordenamiento jurídico.

La misma norma dispone la obligatoriedad del Documento Nacional de Identidad para los mayores de catorce años, salvo en los supuestos en que, conforme a lo previsto en la Ley, haya de ser sustituido por otro documento, y establece también que en el mismo figurarán la fotografía y la firma del titular, así como los datos personales que se determinen reglamentariamente.

En cuanto a la competencia para su expedición y gestión, la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, atribuye al Cuerpo Nacional de Policía, la de la expedición del Documento Nacional de Identidad, al recogerla expresamente entre las funciones que encomienda a este Instituto Policial, el cual la misma Ley dispone que dependerá del Ministerio del Interior.

Por otra parte, la Ley 59/2003, de 19 de diciembre, de firma electrónica, ha venido a atribuir al Documento Nacional de Identidad nuevos efectos y utilidades, como son los de poder acreditar electrónicamente la identidad y demás datos personales del titular que en él consten, así como la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica, cuya incorporación al mismo se establece.

La misma Ley, en el apartado primero de la disposición final segunda dispone que el Gobierno adaptará la regulación reglamentaría del Documento Nacional de Identidad a las previsiones de la referida Ley.

Asimismo, ha de señalarse que la normativa reglamentaria que regula los distintos aspectos del Documento Nacional de Identidad se encuentra dispersa en distintas disposiciones y data, en parte, de fechas anteriores a la vigencia de la Constitución, lo que genera disfunciones a la hora de su aplicación, derivadas tanto de la propia antigüedad de las normas, como de la dispersión de estas.

En este contexto, y a la vista del mandato legal contenido en la Ley 59/2003, antes citada, resulta imprescindible acometer la adecuación y ordenación de la normativa que regula el referido Documento, abordando aquellos aspectos derivados de las nuevas utilidades que se le atribuyen.

En su virtud, a propuesta del Ministro del Interior, con la aprobación previa del Ministro de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros, en su reunión del día 23 de diciembre de 2005,

D I S P O N G O :

Artículo 1. *Naturaleza y funciones.*

1. El Documento Nacional de Identidad es un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes. Su titular estará obligado a la custodia y conservación del mismo.

2. Dicho Documento tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo.

3. A cada Documento Nacional de Identidad, se le asignará un número personal que tendrá la consideración de identificador numérico personal de carácter general.

4. Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En el caso de los españoles menores de edad, o que no gocen de plena capacidad de obrar, el documento nacional de identidad contendrá, únicamente, la utilidad de la identificación electrónica, emitiéndose con el respectivo certificado de autenticación activado.

5. La firma electrónica realizada a través del Documento Nacional de Identidad tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

6. Ningún español podrá ser privado del Documento Nacional de Identidad, ni siquiera temporalmente, salvo en los casos y forma establecidos por las Leyes en los que haya de ser sustituido por otro documento.

Artículo 2. *Derecho y obligación de obtenerlo.*

1. Todos los españoles tendrán derecho a que se les expida el Documento Nacional de Identidad, siendo obligatoria su obtención por los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses.

2. Todas las personas obligadas a obtener el Documento Nacional de Identidad lo están también a exhibirlo cuando fueren requeridas para ello por la Autoridad o sus Agentes.

Artículo 3. *Órgano competente para la expedición y gestión.*

1. Será competencia del Ministerio del Interior el ejercicio de las funciones relativas a la gestión, dirección, organización, desarrollo y administración de todos aquellos aspectos referentes a la expedición y confección del Documento Nacional de Identidad, conforme a lo previsto en la legislación en materia de seguridad ciudadana y de firma electrónica.

2. El ejercicio de las competencias a que se refiere el apartado anterior, incluida la emisión de los certificados de firma electrónica reconocidos, será realizado por la Dirección General de la Policía, a quien corresponderá también la custodia y responsabilidad de los archivos y ficheros, automatizados o no, relacionados con el Documento Nacional de Identidad. A tal efecto, la Dirección General de la Policía quedará sometida a las obligaciones impuestas al responsable del fichero por la Ley Orgánica 15/1999, de 13 de septiembre, de Protección de Datos de Carácter Personal.

Artículo 4. *Procedimiento de expedición.*

1. El Documento Nacional de Identidad se expedirá a solicitud del interesado en la forma y lugares que al efecto se determinen, para lo cual deberá aportar los documentos que se establecen en el artículo 5.1 de este Real Decreto.

2. En orden a facilitar a los ciudadanos la obtención del Documento Nacional de Identidad, el Ministerio del Interior en colaboración con el Ministerio de Administraciones Públicas adoptará las medidas oportunas para el fomento de la cooperación de los distintos órganos de las Administraciones Públicas con la Dirección General de la Policía.

Artículo 5. *Requisitos para la expedición.*

1. Para solicitar la expedición del Documento Nacional de Identidad será imprescindible la presencia física de la persona a quien se haya de expedir, el abono de la tasa legalmente establecida en cada momento y la presentación de los siguientes documentos:

a) Certificación literal de nacimiento expedida por el Registro Civil correspondiente. A estos efectos únicamente serán admitidas las certificaciones expedidas con una antelación máxima de seis meses a la fecha de presentación de la solicitud de expedición del Documento Nacional de Identidad y que contengan la anotación de que se ha emitido a los solos efectos de la obtención de este documento.

b) Una fotografía reciente en color del rostro del solicitante, tamaño 32 por 26 milímetros, con fondo uniforme blanco y liso, tomada de frente con la cabeza totalmente descubierta y sin gafas de cristales oscuros o cualquier otra prenda que pueda impedir o dificultar la identificación de la persona.

c) Certificado o volante de empadronamiento del Ayuntamiento donde el solicitante tenga su domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del documento nacional de identidad.

d) Los españoles residentes en el extranjero acreditarán el domicilio mediante certificación de la Representación Diplomática o Consular donde estén inscritos como residentes.

2. Excepcionalmente, en los supuestos en que, por circunstancias ajenas al solicitante, no pudiera ser presentado alguno de los documentos a que se refiere el apartado primero de este artículo, y siempre que se acrediten por otros medios, suficientes a juicio del responsable del órgano encargado de la expedición, los datos que consten en tales documentos, se le podrá expedir un Documento Nacional de Identidad con la validez que se indica en el artículo siguiente.

3. En el momento de la solicitud, al interesado se le recogerán las impresiones dactilares de los dedos índices de ambas manos. Si no fuere posible obtener la impresión dactilar de alguno de los dedos o de ambos, se sustituirá, en relación con la mano que corresponda, por otro dedo según el siguiente orden de prelación: medio, anular o pulgar; consignándose, en el lugar del soporte destinado a tal fin, el dedo utilizado, o la imposibilidad de obtener alguno de ellos.

Artículo 6. *Validez.*

1. Con carácter general el documento nacional de identidad tendrá un período de validez, a contar desde la fecha de la expedición o de cada una de sus renovaciones, de:

a) Dos años cuando el solicitante no haya cumplido los cinco años de edad.

b) Cinco años, cuando el titular haya cumplido los cinco años de edad y no haya alcanzado los treinta al momento de la expedición o renovación.

c) Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.

d) Permanente cuando el titular haya cumplido los setenta años.

2. De forma excepcional se podrá otorgar validez distinta al Documento Nacional de Identidad en los siguientes supuestos de expedición y renovación:

a) Permanente, a personas mayores de treinta años que acrediten la condición de gran inválido.

b) Por un año en los supuestos del apartado segundo del artículo 5 y del mismo apartado del artículo 7 siempre que, en éste último caso, no se puedan aportar los documentos justificativos que acrediten la variación de los datos.

3. No obstante lo dispuesto en este artículo, en cuanto a la validez de la utilidad informática prevista en el artículo 1.4 se estará a lo que específicamente se establece al respecto en el artículo 12 de este Real Decreto.

Artículo 7. *Renovación.*

1. Transcurrido el período de validez que para cada supuesto se contempla en el artículo anterior, el Documento Nacional de Identidad se considerará caducado y quedarán sin efecto las atribuciones y efectos que le reconoce el ordenamiento jurídico, estando su titular obligado a proceder a la renovación del mismo.

Dicha renovación se llevará a cabo mediante la presencia física del titular del Documento, que deberá abonar la tasa correspondiente y aportar una fotografía con las características señaladas en el artículo 5.1.b). También se le recogerán las impresiones dactilares que se refieren en el apartado tercero del mismo artículo.

2. Independientemente de los supuestos del apartado anterior se deberá proceder a la renovación del Documento Nacional de Identidad en los supuestos de variación de los datos que se recogen en el mismo, en cuyo caso será preciso aportar, además de lo establecido en el apartado anterior, los documentos justificativos que acrediten dicha variación.

Artículo 8. *Expedición de duplicados.*

1. El extravío, sustracción, destrucción o deterioro del Documento Nacional de Identidad, conllevará la obligación de su titular de proveerse inmediatamente de un duplicado, que será expedido en la forma y con los requisitos indicados para la renovación prevista en el apartado primero del artículo anterior. La validez de estos duplicados será la misma que tenían los Documentos a los que sustituyen, salvo que éstos se hallen dentro de los últimos 90 días de su vigencia, en cuyo caso se expedirán con la misma validez que si se tratara de una renovación.

2. Los documentos sustituidos perderán el carácter de Documento Nacional de Identidad, así como los efectos que el ordenamiento jurídico atribuye a éste con respecto a su titular.

Artículo 9. *Entrega del Documento Nacional de Identidad.*

1. La entrega del documento nacional de identidad deberá realizarse personalmente a su titular, y cuando éste sea menor de 14 años o sea una persona con capacidad judicialmente complementada, se llevará a cabo en presencia de quien tenga encomendada la patria potestad o tutela, o persona apoderada por estas últimas. En el momento de la entrega del documento nacional de identidad se proporcionará la información a que se refiere el artículo 18.b) de la Ley 59/2003, de 19 de diciembre.

2. La activación del certificado de firma electrónica en el documento nacional de identidad tendrá carácter voluntario y su utilización se realizará mediante una clave personal y secreta que el titular del documento nacional de identidad podrá introducir reservadamente en el sistema.

3. Al entregar el Documento renovado, se procederá a la retirada del anterior para su inutilización física. Una vez inutilizado podrá ser devuelto a su titular si éste lo solicita.

Artículo 10. *Características de la tarjeta soporte.*

1. El material, formato y diseño de la tarjeta soporte del Documento Nacional de Identidad se determinará por el Ministerio del Interior, teniendo en cuenta en su elaboración la utilización de procedimientos y productos conducentes a la consecución de condiciones de calidad e inalterabilidad y máximas garantías para impedir su falsificación. Llevará incorporado un chip electrónico al objeto de posibilitar la utilidad informática a que se refiere el artículo 1.4 de este Real Decreto.

2. La tarjeta soporte llevará estampados en el anverso, de forma destacada y preeminente los literales «Documento Nacional de Identidad», «España» y «Ministerio del Interior».

Artículo 11. *Contenido.*

1. El Documento Nacional de Identidad recogerá gráficamente los siguientes datos de su titular:

En el anverso:

Apellidos y nombre.
Fecha de nacimiento.
Sexo.
Nacionalidad.
Número personal del Documento Nacional de Identidad y carácter de verificación correspondiente al Número de Identificación Fiscal.
Fotografía.
Firma.

En el reverso:

Lugar de nacimiento.
Provincia-Nación.
Nombre de los padres.
Domicilio.
Lugar de domicilio.
Provincia.
Nación.
Caracteres OCR-B de lectura mecánica.

Los datos de filiación se reflejarán en los mismos términos en que consten en la certificación a la que se alude en el artículo 5.1.a) de este Real Decreto, excepto en el campo de caracteres OCR-B de lectura mecánica, en que por aplicación de acuerdos o convenios internacionales la transcripción literal de aquellos datos impida o dificulte la lectura mecánica y finalidad de aquellos caracteres.

2. Igualmente constarán los siguientes datos referentes al propio Documento y a la tarjeta soporte:

Fecha de caducidad
Número de soporte.

3. Los textos fijos se expresarán en castellano y los expedidos en territorio de aquellas Comunidades Autónomas que tengan otra lengua oficial, serán también expresados en esta.

4. El chip incorporado a la tarjeta soporte contendrá:

Datos de filiación del titular.
Imagen digitalizada de la fotografía.
Imagen digitalizada de la firma manuscrita.
Plantilla de la impresión dactilar del dedo índice de la mano derecha o, en su caso, del que corresponda según lo indicado en el artículo 5.3 de este Real Decreto.
Certificados reconocidos de autenticación y de firma, y certificado electrónico de la autoridad emisora, que contendrán sus respectivos períodos de validez.
Claves privadas necesarias para la activación de los certificados mencionados anteriormente.

Artículo 12. *Validez de los certificados electrónicos.*

1. Con independencia de lo que establece el artículo 6.1 sobre la validez del documento nacional de identidad, la vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a cinco años.

A la extinción de la vigencia del certificado electrónico, podrá solicitarse la expedición de nuevos certificados reconocidos, manteniendo la misma tarjeta del Documento Nacional de Identidad mientras dicho Documento continúe vigente. Para la solicitud de un nuevo certificado deberá mediar la presencia física del titular en la forma y con los requisitos que se determinen por el Ministerio del Interior, de acuerdo con lo previsto en la Ley 59/2003, de 19 de diciembre.

2. El cumplimiento del período establecido en el apartado anterior implicará la inclusión de los certificados en la lista de certificados revocados que será mantenida por la Dirección General de la Policía, bien directamente o a través de las entidades a las que encomiende su gestión.

3. La pérdida de validez del Documento Nacional de Identidad llevará aparejada la pérdida de validez de los certificados reconocidos incorporados al mismo. La renovación del Documento Nacional de Identidad o la expedición de duplicados del mismo implicará, a su vez, la expedición de nuevos certificados electrónicos.

4. También serán causas de extinción de la vigencia del certificado reconocido las establecidas en la Ley 59/2003, de 19 de diciembre, que resulten de aplicación, y, entre otras, el fallecimiento del titular del Documento Nacional de Identidad electrónico.

5. En los supuestos previstos en el artículo 8.1 de este Real Decreto, el titular deberá comunicar inmediatamente tales hechos a la Dirección General de la Policía por los procedimientos y medios que al efecto habilite la misma, al objeto de su revocación.

Artículo 13. *Declaración de Prácticas y Políticas de Certificación.*

De acuerdo y en cumplimiento del artículo 19 de la Ley 59/2003, de 19 de diciembre, el Ministerio del Interior formulará una Declaración de Prácticas y Políticas de Certificación. Dicha Declaración de Prácticas y Políticas de Certificación estará disponible al público de manera permanente y fácilmente accesible en la página de Internet del Ministerio del Interior.

Disposición adicional primera. *Documento de sustitución del Documento Nacional de Identidad en supuestos de retirada de éste.*

En los supuestos en que, de acuerdo con las previsiones establecidas en las Leyes, sea acordada por la Autoridad competente la retirada temporal de Documento Nacional de Identidad por los órganos encargados de la expedición de éste, se procederá a dotar al interesado de un documento identificador que tendrá las características y funcionalidades que determine el Ministerio del Interior, atendiendo a las causas de su retirada.

Disposición adicional segunda. *Documento Nacional de Identidad de los menores de edad.*

La posesión del Documento Nacional de Identidad por los menores de edad no supone, por sí sola, autorización para desplazarse fuera del territorio nacional, debiendo ser suplida, a estos efectos, con la correspondiente autorización de quien ejerza la patria potestad o tutela.

Disposición adicional tercera. *Imposibilidad de expedición o renovación del Documento Nacional de Identidad.*

Cuando exista imposibilidad manifiesta para la expedición del Documento Nacional de Identidad, y sin perjuicio de que por las Autoridades y Órganos correspondientes se compruebe la personalidad del interesado por cualesquiera otros medios, excepcionalmente podrá sustituirse aquél por certificaciones anuales en las que consten los motivos de tal imposibilidad, que en los supuestos de renovación tendrán únicamente el fin de prorrogar la validez del Documento caducado.

Disposición adicional cuarta. *Remisión de información por vía telemática.*

1. La documentación requerida para la expedición del Documento Nacional de Identidad en el artículo 5.1 de este Real Decreto no será exigible cuando sea posible remitir ésta desde los órganos competentes por medios telemáticos a la Dirección General de la Policía, de conformidad con lo que se establezca mediante Convenio.

2. En estos casos, por Orden del Ministro del Interior se establecerá el régimen de aportación de dichos documentos.

Disposición transitoria única. *Validez de los Documentos Nacionales de Identidad expedidos o renovados de conformidad con la normativa anterior a este Real Decreto y proceso de sustitución.*

1. Los Documentos Nacionales de Identidad ya emitidos o los que se continúen expidiendo por el sistema anterior conforme a la normativa existente a la entrada en vigor de este Real Decreto seguirán siendo válidos y eficaces de conformidad con dicha normativa en tanto no se proceda a su sustitución por el Documento Nacional de Identidad de acuerdo con lo que se establece en el apartado siguiente de esta disposición.

2. La Dirección General de la Policía programará y organizará, temporal y territorialmente el proceso de sustitución de las tarjetas soporte del Documento Nacional de Identidad emitidas con anterioridad a la entrada en vigor de este Real Decreto por el nuevo Documento Nacional de Identidad, pudiendo establecerse por razones de interés público programaciones especiales para determinados colectivos.

3. Sólo se podrá solicitar la expedición del nuevo Documento Nacional de Identidad en el marco de la programación a que se hace referencia en el apartado anterior.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas las siguientes disposiciones: Decreto 196/1976, de 6 de febrero, por el que se regula el Documento Nacional de Identidad, y las modificaciones llevadas a cabo en el mismo a través de los Reales Decretos 1189/1978, de 2 de junio; 2002/1979, de 20 de julio; 2091/1982, de 12 de agosto; y 1245/1985, de 17 de julio.

2. Asimismo, quedan derogadas todas aquellas normas de igual o inferior rango que se opongan a lo preceptuado en este Real Decreto.

Disposición final primera. *Título competencial.*

Este Real Decreto se dicta al amparo de las competencias atribuidas al Estado por el artículo 149.1.8.ª,18.ª, 21.ª y 29.ª de la Constitución.

Disposición final segunda. *Desarrollo.*

1. El Ministerio del Interior adoptará las disposiciones necesarias para dar cumplimiento a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, en materia de creación y modificación de ficheros de titularidad pública.

2. Se habilita a los Ministros del Interior, de Justicia, de Economía y Hacienda, de Industria, Turismo y Comercio y de Administraciones Públicas para que dicten, en el ámbito de sus respectivas competencias, cuantas disposiciones sean necesarias para el desarrollo y aplicación de este Real Decreto.

Disposición final tercera. *Tasas.*

El Gobierno promoverá la norma legal de rango adecuado para la adecuación de la tasa que haya de percibirse por la expedición del Documento Nacional de Identidad, de acuerdo con su coste y en consideración a los beneficios que proporciona a la comunidad.

Disposición final cuarta. *Entrada en vigor.*

El presente Real Decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», excepto lo relativo al artículo 1.4 que entrará en vigor cuando lo haga el nuevo formato y diseño del Documento Nacional de Identidad.

§ 14

Orden ISM/189/2021, de 3 de marzo, por la que se regula el Registro electrónico de apoderamientos de la Seguridad Social

Ministerio de Inclusión, Seguridad Social y Migraciones
«BOE» núm. 55, de 5 de marzo de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-3421

Mediante la Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social, para la realización de trámites y actuaciones por medios electrónicos, dicho registro se configura como medio para acreditar la representación otorgada a tal efecto a que se refiere el artículo 129.2 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre.

Posteriormente, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, ha establecido una regulación completa y sistemática de las relaciones «ad extra» entre las administraciones públicas y los administrados, cuya finalidad principal es la simplificación y agilización de los procedimientos administrativos.

A este respecto, la referida Ley 39/2015, de 1 de octubre, dedica su título I a los interesados en el procedimiento, en el que, tras regular en su artículo 3 la capacidad de obrar para actuar ante las administraciones públicas a los efectos previstos en dicha ley, prevé en materia de representación nuevos instrumentos para su acreditación en el ámbito exclusivo de las administraciones públicas, regulando especialmente en sus artículos 5 y 6 el apoderamiento «apud acta», presencial o electrónico, y la acreditación de su inscripción en el registro electrónico de apoderamientos de la administración pública competente.

Por su parte, en el citado artículo 6 se establece la información mínima que deben contener los asientos que se realicen en los registros electrónicos de apoderamientos, ya sean generales o particulares, y se indica que los poderes que se inscriban en esos registros electrónicos deberán corresponder a alguna de las tres categorías siguientes:

En primer lugar, los poderes generales para que el apoderado pueda realizar en nombre del poderdante cualquier actuación administrativa y ante cualquier administración pública.

En segundo lugar, los poderes que permiten al apoderado actuar en nombre del poderdante para cualquier actuación administrativa ante una administración u organismo concreto.

En tercer lugar, los poderes que permiten al apoderado actuar en nombre del poderdante únicamente para la realización de determinados trámites especificados en el poder.

En este ámbito, el mismo artículo 6 de la Ley 39/2015, de 1 de octubre, prevé que los registros electrónicos generales de apoderamientos no impedirán la existencia de registros electrónicos particulares en cada organismo, donde se inscribirán los poderes otorgados

para la realización de actuaciones generales o trámites específicos ante el mismo. También prevé la interoperabilidad entre los registros electrónicos generales y particulares de apoderamientos a fin de constituir un instrumento válido de comprobación y acreditación de la representación de un tercero ante las administraciones públicas, bastando para ello no solo con la mera consulta electrónica de los datos contenidos en otros registros administrativos similares, sino también con la consulta al registro mercantil, al de la propiedad o al de los correspondientes protocolos notariales.

En atención a tales previsiones legales y en el marco del impulso al empleo de los medios electrónicos, informáticos y telemáticos en las relaciones entre la Administración de la Seguridad Social y los ciudadanos, mediante esta orden se procede a dar una nueva regulación al Registro electrónico de apoderamientos de la Seguridad Social, creado y regulado hasta este momento por la Orden ESS/486/2013, de 26 de marzo.

La nueva regulación del Registro electrónico de apoderamientos de la Seguridad Social viene motivada por la necesidad de desarrollar en dicho ámbito las previsiones que sobre la materia contiene la ya citada Ley 39/2015, de 1 de octubre, tanto en su artículo 5, acerca de los requisitos que han de cumplir los apoderamientos, en sus distintas modalidades, para poder ser inscritos en los registros electrónicos de las diferentes administraciones públicas, como en su artículo 6, respecto de la necesaria incorporación al referido Registro electrónico de los apoderamientos que se efectúen dentro de su ámbito competencial.

Esta orden se adecua a los principios de buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre.

Así, la norma es respetuosa con los principios de necesidad, eficacia y proporcionalidad, en tanto que con ella se persigue el fin pretendido, consistente en acomodar la regulación del Registro electrónico de apoderamientos de la Seguridad Social a las previsiones contenidas al respecto en la mencionada Ley 39/2015, de 1 de octubre, al objeto de asegurar la efectiva aplicación de lo establecido en este ámbito en sus artículos 5 y 6, no tratándose de una norma restrictiva de derechos, sino garante de los mismos.

Asimismo, su regulación cumple los principios de seguridad jurídica y eficiencia, al ser coherente con el resto del ordenamiento jurídico, estar sus objetivos claramente definidos y responder a la finalidad de mejorar el servicio público, al permitir a los interesados formalizar apoderamientos y acreditar representaciones en favor de terceros, no imponiéndoles nuevas cargas administrativas.

Finalmente, la orden se ajusta al principio de transparencia puesto que, de acuerdo con lo establecido en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno, se ha sometido al trámite de audiencia e información pública.

La orden ha sido informada favorablemente por la Comisión Ministerial de Administración Digital, conforme a lo establecido por el artículo 2.2.h) de la Orden ESS/1355/2015, de 25 de junio, por la que se creó dicho órgano colegiado en el entonces Ministerio de Empleo y Seguridad Social y se reguló su composición y funciones.

También ha sido informada por la Agencia Española de Protección de Datos, de acuerdo con lo previsto en el artículo 5.b) del Estatuto de la indicada Agencia, aprobado por el Real Decreto 428/1993, de 26 de marzo.

Esta orden se dicta en ejercicio de la habilitación conferida al Ministerio de Inclusión, Seguridad Social y Migraciones por el artículo 5.2.b) y la disposición final octava del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre, y de acuerdo con la competencia exclusiva en materia de legislación básica de la Seguridad Social que el artículo 149.1.17.ª de la Constitución Española atribuye al Estado.

En su virtud, con la aprobación previa de la Ministra de Política Territorial y Función Pública y de acuerdo con el Consejo de Estado, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Esta orden tiene por objeto regular los requisitos y condiciones de funcionamiento del Registro electrónico de apoderamientos de la Seguridad Social (en adelante el registro), en el que se inscribirán los apoderamientos que de forma voluntaria se otorguen «apud acta» a favor de un tercero, presencial o electrónicamente, por quien ostente la condición de

interesado en un procedimiento administrativo, para actuar en su nombre ante la Administración de la Seguridad Social.

2. El registro no tiene carácter público, será único en el ámbito de la Administración de la Seguridad Social y estará accesible en la sede electrónica de la Secretaría de Estado de la Seguridad Social y Pensiones (en adelante SEDESS).

3. Las representaciones legales no serán objeto de inscripción en el registro.

4. A los efectos de esta orden, se entiende por Administración de la Seguridad Social la totalidad de las direcciones generales, entidades gestoras y servicios comunes incluidos en el ámbito de aplicación de la SEDESS, de conformidad con el artículo 2.a) de la Orden TIN/1459/2010, de 28 de mayo, por la que se crea la sede electrónica de la Secretaría de Estado de la Seguridad Social.

Artículo 2. *Tipos de apoderamientos a inscribir en el registro.*

En el registro podrán inscribirse los siguientes tipos de apoderamientos:

a) Apoderamiento general, para que el apoderado pueda llevar a cabo en nombre del poderdante cualquier actuación administrativa en todas las materias, trámites y grupos de trámites recogidos en el anexo I, sin que se pueda renunciar o revocar el poder por separado respecto a alguno de ellos.

b) Apoderamiento por materias, para que el apoderado pueda actuar en nombre del poderdante y llevar a cabo cualquiera de los trámites y/o grupos de trámites en la materia seleccionada de entre las relacionadas en el anexo I, sin que se pueda renunciar o revocar el poder por separado respecto a alguno de estos trámites.

c) Apoderamiento por trámites y/o grupos de trámites, para que el apoderado pueda actuar en nombre del poderdante solo en aquellos trámites y/o grupos de trámites seleccionados de entre los relacionados en el anexo I, pudiéndose renunciar o revocar el poder por separado respecto a cualquiera de ellos.

Artículo 3. *Órganos competentes.*

1. Corresponde a la Secretaría de Estado de la Seguridad Social y Pensiones la titularidad y gestión del registro, así como la aprobación y modificación de los modelos que resulten precisos para su adecuada gestión.

2. Corresponde a la Gerencia de Informática de la Seguridad Social garantizar la disponibilidad y accesibilidad del registro; la identificación de los interesados mediante métodos de identificación admitidos en la SEDESS; la integridad de los datos incorporados; la generación de evidencias electrónicas que permitan la constatación de la fecha y hora de los accesos y actuaciones relevantes para la incorporación de tales datos, así como la generación de documentos electrónicos que acrediten los poderes inscritos en el registro.

Artículo 4. *Poderdantes y apoderados.*

1. Podrán otorgar apoderamiento las personas físicas, jurídicas y entidades sin personalidad jurídica que ostenten capacidad de obrar y que tengan la condición de interesados en relación con las materias, trámites y/o grupos de trámites relacionados en el anexo I.

2. Podrán ser apoderados las personas físicas que ostenten capacidad de obrar, así como las personas jurídicas cuando, además, tengan prevista en sus estatutos la posibilidad de actuar en representación de un tercero ante las administraciones públicas.

Artículo 5. *Apoderamientos. Otorgamiento y otras actuaciones.*

1. A efectos de su inscripción en el registro, los apoderamientos que se otorguen «apud acta» podrán efectuarse de las siguientes formas:

a) Mediante comparecencia electrónica en la SEDESS, a través del uso de los métodos de identificación y firma admitidos en ella.

Si el compareciente fuese una persona jurídica o una entidad sin personalidad jurídica, la identificación y firma se realizarán mediante el uso de certificados cualificados de

representante, como medio de acreditar la representación y capacidad para realizar las actuaciones en el registro.

b) Mediante comparecencia de la persona física en las oficinas de asistencia en materia de registros de la Seguridad Social, donde el compareciente, una vez identificado por el funcionario habilitado, firmará la correspondiente solicitud.

c) Mediante comparecencia de la persona física en las oficinas de asistencia en materia de registros de otras administraciones públicas u organismos, para la posterior remisión del poder al Registro electrónico de apoderamientos de la Seguridad Social.

2. La modificación de los datos y de la vigencia de los apoderamientos otorgados, así como la consulta sobre sus términos y situación y las demás actuaciones relativas a los mismos reguladas en esta orden, tales como su aceptación, renuncia y revocación, podrán llevarse a cabo, asimismo, en las formas señaladas en el apartado anterior.

Artículo 6. *Inscripción de los apoderamientos.*

1. El poderdante podrá solicitar la inscripción en el registro del apoderamiento otorgado en las formas previstas en el artículo 5.

2. Desde el registro se comunicará al apoderado el otorgamiento del poder a su favor, advirtiéndole, cuando proceda, de la necesidad de presentar la declaración responsable a que se refiere el apartado 4 de este artículo y de aceptar expresamente el apoderamiento en los supuestos a que se refiere el artículo 9.

A efectos de la comunicación indicada en el párrafo anterior, el poderdante deberá facilitar los datos de contacto del apoderado.

3. Los poderes surtirán efectos ante la Administración de la Seguridad Social desde la fecha de su inscripción en el registro y respecto de las materias, trámites y/o grupos de trámites a los que expresamente se refieran y que hayan sido seleccionados de entre los relacionados en el anexo I y publicados en la SEDESS.

4. Los poderes otorgados en favor de personas jurídicas no se inscribirán ni surtirán efecto hasta que aquellas procedan a presentar una declaración responsable manifestando que, en sus estatutos, está prevista la posibilidad de representar a terceros ante las administraciones públicas.

Esa declaración deberá firmarse electrónicamente en el plazo máximo de un mes a contar desde la presentación de la solicitud de inscripción del poder en el registro. En caso de presentarse nuevas solicitudes de registro de apoderamientos a favor de la misma persona jurídica, no será necesaria la presentación de una nueva declaración responsable, siempre y cuando se mantengan los requisitos de capacidad que la sustentan.

La declaración responsable sustituirá a la presentación de los estatutos, sin perjuicio de que estos puedan ser exigidos con posterioridad por el órgano, entidad gestora o servicio común competente. En este último caso deberá constar en el registro el resultado de la comprobación realizada.

5. Los apoderamientos que necesiten aceptación expresa por parte del apoderado no se inscribirán ni surtirán efecto hasta que se produzca dicha aceptación, en los términos señalados en el artículo 9.

Artículo 7. *Contenido del registro.*

1. El registro estará disponible en la SEDESS, donde se mantendrá una relación pública y actualizada de todas las materias, trámites y/o grupos de trámites competencia de la Administración de la Seguridad Social, que pueden ser objeto de apoderamiento.

2. En los asientos que se realicen para inscribir un apoderamiento en el registro se harán constar los siguientes datos:

a) Nombre y apellidos o denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del poderdante, así como sus datos de contacto.

b) Nombre y apellidos o denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del apoderado, así como sus datos de contacto.

c) Materias, trámites y/o grupos de trámites objeto de apoderamiento.

d) Periodo de vigencia del poder.
e) Número de referencia del poder asignado por el registro.
f) Fecha de inscripción en el registro.
g) Estado del poder.
h) Tipo de poder según las facultades que otorgue.

Artículo 8. *Plazo de vigencia de los apoderamientos inscritos en el registro.*

1. Los poderes inscritos en el registro tendrán una vigencia máxima de cinco años, a contar desde la fecha de su inscripción.
2. En cualquier momento antes de la finalización del plazo señalado en el apartado anterior el poderdante podrá modificar, revocar o prorrogar la vigencia del apoderamiento, en cuyo caso podrá solicitar la modificación de su plazo de vigencia en las formas previstas en el artículo 5.
3. Las prórrogas otorgadas por el poderdante tendrán una validez determinada, sin que esta pueda ser superior a cinco años contados desde la fecha de inscripción de la prórroga en el registro.

Artículo 9. *Aceptación expresa del apoderamiento.*

1. La aceptación expresa del apoderado resultará necesaria en los supuestos en los que el apoderamiento comprenda la recepción de comunicaciones o notificaciones, sea cual sea la naturaleza del procedimiento.
2. El apoderado deberá aceptar expresamente el apoderamiento en el plazo máximo de un mes desde su otorgamiento, en las formas previstas en el artículo 5.

En estos casos, el apoderamiento solo se inscribirá y surtirá efectos desde la fecha en que conste esa aceptación en el registro.

Artículo 10. *Renuncia y revocación del apoderamiento.*

La renuncia por el apoderado a un apoderamiento inscrito en el registro y la revocación de este por el poderdante, efectuadas en las formas previstas en el artículo 5, solo surtirán efectos desde la fecha en que se produzca la inscripción de la renuncia o la revocación en el registro.

Artículo 11. *Consulta al registro por parte de los interesados y obtención de certificados de poderes registrados.*

Los interesados podrán consultar de forma electrónica los datos relativos a la inscripción, contenido y vigencia del poder o poderes inscritos en los que figuren como poderdantes o apoderados, así como obtener certificados de los apoderamientos inscritos en el registro.

Artículo 12. *Protección de datos de carácter personal.*

En materia de protección de datos el registro se ajustará a lo previsto al respecto en la normativa española y europea directamente aplicable sobre protección de datos personales.

Artículo 13. *Aprobación de modelos.*

1. Se aprueban los siguientes modelos inscribibles en el registro, en función de los distintos tipos de apoderamientos a que se refiere el artículo 2 y de las actuaciones a realizar respecto a ellos:

a) Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de cualquier trámite en todas o en algunas de las materias relacionadas en el anexo I, y que figura como anexo II.
b) Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de determinados trámites, de entre los relacionados en el anexo I, y que figura como anexo III.
c) Aceptación, renuncia y revocación de poderes otorgados, que figura como anexo IV.
d) Modificación del plazo de vigencia, que figura como anexo V.

2. Cuando la comparecencia personal tenga lugar en las oficinas de asistencia en materia de registros de otra administración pública u organismo a que se refiere el artículo 5.1.c), los modelos indicados en el apartado anterior serán presentados en dicho registro para su envío, vía intercambio registral, a la Administración de la Seguridad Social, a efectos de su posterior inclusión en el Registro electrónico de apoderamientos de la Seguridad Social.

Disposición adicional primera. *Representación en el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social.*

La representación otorgada en el ámbito del Sistema de remisión electrónica de datos (Sistema RED) se regirá por su propia normativa.

Disposición adicional segunda. *Documentos normalizados de representación en materia de prestaciones.*

Los documentos normalizados de representación aprobados por las entidades gestoras al amparo del artículo 129.2 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto Legislativo 8/2015, de 30 de octubre, para su uso en los procedimientos dirigidos al reconocimiento de prestaciones de la Seguridad Social, seguirán siendo válidos, si bien no serán objeto de inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

Disposición adicional tercera. *No incremento de gasto público.*

Esta orden no implica incremento de dotaciones o retribuciones, ni de gasto de personal, ni de cualesquiera otros gastos a cargo del sector público. Asimismo, no supone disminución de ingreso alguno para la Hacienda Pública Estatal y se llevará a cabo con las disponibilidades presupuestarias existentes.

Disposición transitoria única. *Vigencia de anteriores apoderamientos.*

Los apoderamientos otorgados al amparo de la Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social para la realización de trámites y actuaciones por medios electrónicos, perderán su validez el 2 de abril de 2021 si antes de esa fecha no han sido adaptados a la regulación de esta orden, mediante la cumplimentación de los nuevos modelos de poderes a que se refiere su artículo 13.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden ESS/486/2013, de 26 de marzo, por la que se crea y regula el Registro electrónico de apoderamientos de la Seguridad Social para la realización de trámites y actuaciones por medios electrónicos.

Disposición final primera. *Título competencial.*

Esta orden se dicta al amparo de lo dispuesto en el artículo 149.1.17.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de legislación básica de la Seguridad Social.

Disposición final segunda. *Facultades de aplicación.*

Se habilita al titular de la Secretaría de Estado de la Seguridad Social y Pensiones para dictar cuantas resoluciones resulten necesarias para la aplicación y ejecución de lo previsto en esta orden y para actualizar sus anexos.

Disposición final tercera. *Entrada en vigor.*

La presente orden entrará en vigor el día 2 de abril de 2021.

ANEXO I

Relación de materias, trámites y grupos de trámites susceptibles de apoderamiento

Materia	Trámites
Todas las gestiones con la Seguridad Social.	Todos los trámites con la Seguridad Social.
Prestaciones.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Inscripción, afiliación, cotización y recaudación.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Sanidad marítima.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Formación marítima y sanitaria.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Contratación.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Patrimonio.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Auditoría.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.
Reclamaciones y recursos.	Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones.
Procedimientos de la Dirección General de Ordenación de la Seguridad Social.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.
	Recibir notificaciones y comunicaciones.

Materia	Descripción
Todas las gestiones con la Seguridad Social.	El apoderado podrá realizar todas las actuaciones en cualquier materia y trámite ante la Seguridad Social.
Prestaciones.	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones de la Seguridad Social, incluidas las prestaciones específicas previstas para los trabajadores del mar, así como para su revalorización, revisión, mantenimiento y, en su caso, extinción. Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos sancionadores en materia de prestaciones de la Seguridad Social.
Inscripción, afiliación, cotización y recaudación.	El apoderado podrá realizar actuaciones relativas a los procedimientos y servicios de inscripción, baja y variación de datos de las empresas en la Seguridad Social; el alta, baja y variación de datos de los trabajadores, así como la cotización y la recaudación de los recursos de la Seguridad Social, incluidas las actas de liquidación e infracción competencia de la Tesorería General de la Seguridad Social.
Sanidad marítima.	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones y servicios relacionados con la sanidad preventiva y asistencial que realiza el Instituto Social de la Marina para el sector marítimo pesquero, como reconocimientos médicos de aptitud, inspección de las condiciones sanitarias de los buques, inspección de botiquines a bordo, ayudas para la dotación de botiquines, asistencia sanitaria a bordo y en el extranjero y vigilancia de la salud.
Formación marítima y sanitaria.	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites relacionados con la formación profesional marítima y sanitaria prestada por el Instituto Social de la Marina.
Contratación.	El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por la Administración de la Seguridad Social.
Patrimonio.	El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con la Tesorería General de la Seguridad Social.
Auditoría.	El apoderado podrá realizar actuaciones en relación a las auditorías públicas que sobre las mutuas y las empresas colaboradoras con la Seguridad Social lleva a cabo la Intervención General de la Seguridad Social, así como respecto a las actuaciones de control financiero de ayudas y subvenciones realizadas por el citado órgano de control.
Reclamaciones y recursos.	El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por la Administración de la Seguridad Social.
Procedimientos de la Dirección General de Ordenación de la Seguridad Social.	El apoderado podrá realizar todas las actuaciones relacionadas con los procedimientos competencia de la Dirección General de Ordenación de la Seguridad Social.

Trámite	Descripción
Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	El apoderado puede presentar, subsanar o completar solicitudes, escritos, declaraciones y comunicaciones, acompañando, en su caso, los documentos acreditativos requeridos o que considere oportunos. También puede desistir de las solicitudes presentadas. Igualmente puede aportar a un procedimiento administrativo datos, documentos y elementos de prueba, formular alegaciones y, en su caso, participar en el trámite de audiencia. Asimismo, puede realizar cualquier otro trámite o actuación administrativa prevista en la legislación aplicable, incluido el abono de una obligación o el cobro de una cantidad líquida.
Recibir notificaciones y comunicaciones.	El apoderado puede recibir las notificaciones de resolución o actos administrativos que ponen fin a los procedimientos o que implican efectos jurídicos y cuya fecha de recepción por parte del interesado marca el inicio del plazo para poder presentar reclamaciones o recursos. Asimismo, puede recibir todas aquellas comunicaciones informativas, sin efectos jurídicos, que la entidad que gestiona el procedimiento pueda remitir al interesado. El apoderamiento de este trámite implica que las notificaciones y/o comunicaciones se realizarán por vía electrónica al apoderado, conforme a la regulación específica de dicha materia.
Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones.	El apoderado puede presentar escritos de reclamación y recursos contra resoluciones y actos de trámite en los casos legalmente previstos, intervenir en todos sus trámites, formular alegaciones y desistir de los mismos, así como recibir las notificaciones y comunicaciones que puedan generarse respecto a los recursos y reclamaciones formulados.

ANEXO II

Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de cualquier trámite en todas o en algunas de las materias que se especifican

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Teléfono:	Correo electrónico:
Domicilio:		
Código Postal:	Localidad:	Provincia:

☐ Persona jurídica o entidad sin personalidad jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Identificación del representante:		
Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		
Identificación de la persona jurídica:		
NIF:	Razón Social:	
Teléfono:	Correo electrónico:	

****

El poderdante otorga poder a favor de (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Correo electrónico:	

☐ Persona jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

NIF:	Razón Social:
Correo electrónico:	

Poder

Tan amplio y bastante como en Derecho sea necesario para actuar en nombre del poderdante para la realización de cualquier trámite en las materias seleccionadas a continuación

Elija una de las dos opciones siguientes:

☐ Materia general que abarca todas las gestiones con la Seguridad Social.

☐ Materia(s) concreta(s) incluidas en el ámbito de la Seguridad Social (elija una o varias opciones):

	Materia	Descripción
☐	Prestaciones	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones de la Seguridad Social, incluidas las prestaciones específicas previstas para los trabajadores del mar, así como para su revalorización, revisión, mantenimiento y, en su caso, extinción. Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos sancionadores en materia de prestaciones de la Seguridad Social.
☐	Inscripción, afiliación, cotización y recaudación	El apoderado podrá realizar actuaciones relativas a los procedimientos y servicios de inscripción, baja y variación de datos de las empresas en la Seguridad Social; el alta, baja y variación de datos de los trabajadores, así como la cotización y la recaudación de los recursos de la Seguridad Social, incluidas las actas de liquidación e infracción competencia de la Tesorería General de la Seguridad Social.
☐	Sanidad marítima	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones y servicios relacionados con la sanidad preventiva y asistencial que realiza el Instituto Social de la Marina para el sector marítimo pesquero, como reconocimientos médicos de aptitud, inspección de las condiciones sanitarias de los buques, inspección de botiquines a bordo, ayudas para la dotación de botiquines, asistencia sanitaria a bordo y en el extranjero y vigilancia de la salud.
☐	Formación marítima y sanitaria	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites relacionados con la formación profesional marítima y sanitaria prestada por el Instituto Social de la Marina.
☐	Contratación	El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por la Administración de la Seguridad Social.
☐	Patrimonio	El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con la Tesorería General de la Seguridad Social.
☐	Auditoría	El apoderado podrá realizar actuaciones en relación a las auditorías públicas que sobre las mutuas y las empresas colaboradoras con la Seguridad Social lleva a cabo la Intervención General de la Seguridad Social, así como respecto a las actuaciones de control financiero de ayudas y subvenciones realizadas por el citado órgano de control.
☐	Reclamaciones y recursos	El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por la Administración de la Seguridad Social.
☐	Procedimientos de la Dirección General de Ordenación de la Seguridad Social	El apoderado podrá realizar todas las actuaciones relacionadas con los procedimientos competencia de la Dirección General de Ordenación de la Seguridad Social.

Vigencia del poder:

Fecha de fin: A rellenar por el poderdante / /	La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

En _____, ____/____/____ Firma del poderdante:
Lugar Fecha

ANEXO III

Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante la Administración de la Seguridad Social de determinados trámites

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Teléfono:	Correo electrónico:
Domicilio:		
Código Postal:	Localidad:	Provincia:

☐ Persona jurídica o entidad sin personalidad jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Identificación del representante:		
Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		
Identificación de la persona jurídica:		
NIF:	Razón Social:	
Teléfono:	Correo electrónico:	

****

El poderdante otorga poder a favor de (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Correo electrónico:	

☐ Persona jurídica que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

NIF:	Razón Social:
Correo electrónico:	

Poder

Tan amplio y bastante como en Derecho sea necesario para actuar en nombre del poderdante para la realización de los trámites seleccionados a continuación (elija una o varias opciones)

Materia*	Trámites*	
Prestaciones	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Inscripción, afiliación, cotización y recaudación	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Sanidad marítima	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Formación marítima y sanitaria	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Contratación	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Patrimonio	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Auditoría	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Reclamaciones y recursos	Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones.	☐
Procedimientos de la Dirección General de Ordenación de la Seguridad Social	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐

**NOTA: Consulte la descripción de materias y trámites al final de este formulario.*

Vigencia del poder:

Fecha de fin: A rellenar por el poderdante / /	La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

En _____, ____/____/____ Firma del poderdante:
Lugar Fecha

Materia	Descripción
Todas las gestiones con la Seguridad Social	El apoderado podrá realizar todas las actuaciones en cualquier materia y trámite ante la Seguridad Social.
Prestaciones	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones de la Seguridad Social, incluidas las prestaciones específicas previstas para los trabajadores del mar, así como para su revalorización, revisión, mantenimiento y, en su caso, extinción. Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos sancionadores en materia de prestaciones de la Seguridad Social.
Inscripción, afiliación, cotización y recaudación	El apoderado podrá realizar actuaciones relativas a los procedimientos y servicios de inscripción, baja y variación de datos de las empresas en la Seguridad Social; el alta, baja y variación de datos de los trabajadores, así como la cotización y la recaudación de los recursos de la Seguridad Social, incluidas las actas de liquidación e infracción competencia de la Tesorería General de la Seguridad Social.
Sanidad marítima	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento y conservación del derecho a las prestaciones y servicios relacionados con la sanidad preventiva y asistencial que realiza el Instituto Social de la Marina para el sector marítimo pesquero, como reconocimientos médicos de aptitud, inspección de las condiciones sanitarias de los buques, inspección de botiquines a bordo, ayudas para la dotación de botiquines, asistencia sanitaria a bordo y en el extranjero y vigilancia de la salud.
Formación marítima y sanitaria	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites relacionados con la formación profesional marítima y sanitaria prestada por el Instituto Social de la Marina.
Contratación	El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por la Administración de la Seguridad Social.
Patrimonio	El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con la Tesorería General de la Seguridad Social.
Auditoría	El apoderado podrá realizar actuaciones en relación a las auditorías públicas que sobre las mutuas y las empresas colaboradoras con la Seguridad Social lleva a cabo la Intervención General de la Seguridad Social, así como respecto a las actuaciones de control financiero de ayudas y subvenciones realizadas por el citado órgano de control.
Reclamaciones y recursos	El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por la Administración de la Seguridad Social.
Procedimientos de la Dirección General de Ordenación de la Seguridad Social	El apoderado podrá realizar todas las actuaciones relacionadas con los procedimientos competencia de la Dirección General de Ordenación de la Seguridad Social.

Trámites	Descripción
Presentar solicitudes, realizar alegaciones o aportar elementos de prueba	El apoderado puede presentar, subsanar o completar solicitudes, escritos, declaraciones y comunicaciones, acompañando, en su caso, los documentos acreditativos requeridos o que considere oportunos. También puede desistir de las solicitudes presentadas. Igualmente puede aportar a un procedimiento administrativo datos, documentos y elementos de prueba, formular alegaciones y, en su caso, participar en el trámite de audiencia. Asimismo, puede realizar cualquier otro trámite o actuación administrativa prevista en la legislación aplicable, incluido el abono de una obligación o el cobro de una cantidad líquida.
Recibir notificaciones y comunicaciones	El apoderado puede recibir las notificaciones de resolución o actos administrativos que ponen fin a los procedimientos o que implican efectos jurídicos y cuya fecha de recepción por parte del interesado marca el inicio del plazo para poder presentar reclamaciones o recursos. Asimismo, puede recibir todas aquellas comunicaciones informativas, sin efectos jurídicos, que la entidad que gestiona el procedimiento pueda remitir al interesado. El apoderamiento de este trámite implica que las notificaciones y/o comunicaciones se realizarán por vía electrónica al apoderado, conforme a la regulación específica de dicha materia.
Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones	El apoderado puede presentar escritos de reclamación y recursos contra resoluciones y actos de trámite en los casos legalmente previstos, intervenir en todos sus trámites, formular alegaciones y desistir de los mismos, así como recibir las notificaciones y comunicaciones que puedan generarse respecto a los recursos y reclamaciones formulados.

ANEXO IV

Aceptación, renuncia y revocación de poderes otorgados

Elija solo una de las siguientes operaciones:

Poderdante

☐ Revocación de poder(es).

Apoderado

☐ Aceptación de poder(es).

☐ Renuncia de poder(es).

****

Identificación del compareciente:

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		

☐ Persona jurídica o entidad sin personalidad jurídica -como poderdante- que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Identificación del representante:		
Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		
Identificación de la persona jurídica:		
NIF:	Razón Social:	

****

Indique a continuación los poderes afectados por la operación seleccionada separados por comas.

Número de referencia de los poderes:

Efectos de la operación desde la fecha de inscripción
en el Registro electrónico de apoderamientos de la Seguridad Social.

En _____, ____/____/____ Firma del compareciente:

ANEXO V

Modificación de plazo de poderes otorgados

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Nombre:		Primer apellido:	Segundo apellido:
	DNI/NIF/Documento equivalente:		

☐ Persona jurídica o entidad sin personalidad jurídica -como poderdante- que ostente capacidad de obrar ***(todos los datos son obligatorios)***:

Identificación del representante:		
Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		
Identificación de la persona jurídica:		
NIF:	Razón Social:	

****

Indique a continuación los poderes afectados (una línea para cada poder).
La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

Número de referencia de los poderes:	**Fecha de fin de los poderes (día/mes/año):**
	/ /
	/ /
	/ /
	/ /
	/ /
	/ /
	/ /
	/ /

Efectos de la operación desde la fecha de inscripción
en el Registro electrónico de apoderamientos de la Seguridad Social.

En _____, ____/____/____ Firma del compareciente:

§ 15

Orden PRE/1838/2014, de 8 de octubre, por la que se publica el Acuerdo de Consejo de Ministros, de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas

Ministerio de la Presidencia
«BOE» núm. 245, de 9 de octubre de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-10264

El Consejo de Ministros, en su reunión de 19 de septiembre de 2014 y a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia y de los Ministros de Hacienda y Administraciones Públicas, del Interior, de Empleo y Seguridad Social y de Industria, Energía y Turismo, ha adoptado un Acuerdo por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas.

En virtud de lo dispuesto en el apartado séptimo del citado Acuerdo y para general conocimiento, se dispone su publicación como Anexo a la presente Orden.

ANEXO

Acuerdo de Consejo de Ministros por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas

El Gobierno de España ha puesto en marcha un ambicioso proyecto reformista encaminado a corregir los desequilibrios que frenan nuestro crecimiento y crear las bases idóneas sobre las que levantar un nuevo ciclo de prosperidad económica y empleo.

Sobre estas premisas, el 26 de octubre de 2012 el Consejo de Ministros aprobó un Acuerdo por el que se crea la Comisión para la Reforma de las Administraciones Públicas (CORA) y tras la presentación de su Informe en el Consejo de Ministros de 21 de junio de 2013, se iniciaron actuaciones para simplificar los procedimientos y reducir las cargas administrativas para ciudadanos y empresas y para evitar solapamientos y duplicidades en las actuaciones de las Administraciones, propiciando la gestión de servicios y medios comunes con el objetivo de mejorar la eficacia de la actividad pública con ahorro de costes.

En el ámbito de los medios informáticos, las medidas propuestas por el Informe CORA se han centrado en una racionalización de las actuales estructuras organizativas en el ámbito de las Tecnologías de la Información y de las Comunicaciones (TIC) del Sector Público Administrativo Estatal, consolidando infraestructuras y servicios comunes que

permitan hacer una utilización más eficiente de los recursos tecnológicos, así como ofrecer mayores niveles de calidad en los servicios prestados.

Con el fin de desarrollar los procesos de estandarización que considera esenciales para incentivar la compartición y reutilización de las infraestructuras y servicios, el informe CORA contempló la creación de un órgano específico, al más alto nivel, que impulsara y coordinara el necesario proceso de racionalización de las diversas facetas de la política de tecnologías de la información y de comunicaciones en todo el ámbito del Sector Público Administrativo Estatal: adquisiciones de bienes informáticos, estructura de redes, servicios de administración electrónica y optimización de los sistemas de publicación web. Este órgano es la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado.

En desarrollo del informe CORA, las competencias para la coordinación del proceso de racionalización de las TIC en el Sector Público Administrativo Estatal se atribuyeron inicialmente al Ministerio de la Presidencia de acuerdo con lo dispuesto en el Real Decreto 695/2013, de 20 de septiembre. Este Real Decreto, atribuyó a la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado la elaboración, coordinación y dirección de la estrategia sobre tecnologías de la información y de las comunicaciones del Sector Público Administrativo Estatal, así como la planificación de la consolidación de las infraestructuras y servicios horizontales en el ámbito de la Administración Electrónica, entre otras. Por Real Decreto 802/2014, de 19 de septiembre, se atribuyen al Ministerio de Hacienda y Administraciones Públicas estas competencias y se adscribe a este Ministerio la Dirección de Tecnologías de la Información y las Comunicaciones dependiendo de la Secretaría de Estado de Administraciones Públicas.

En este modelo de gestión común e integrada, facilitadora de las relaciones entre sociedad y Administración, resulta esencial habilitar un sistema simple, rápido y seguro de identificación, autenticación y firma de los ciudadanos en su relación electrónica con los prestadores de servicios del Sector Público Administrativo Estatal y, en la medida que así se acuerde, del resto del Sector Público Estatal, de las Administraciones Autonómicas y Entidades Locales. Además, este sistema de identificación y autenticación electrónicas debe permitir la expresión de la voluntad del usuario, cuando así lo requiera el servicio o trámite electrónico, por medio de los sistemas de firma electrónica válidos según la normativa vigente.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, supuso que las Administraciones Públicas hicieran un enorme esfuerzo para poner todos sus servicios a disposición de la ciudadanía por medios electrónicos y hacerlo con las mayores garantías de seguridad posibles. Los altos niveles de seguridad previstos para el acceso electrónico a los servicios se han apoyado principalmente en los sistemas de firma electrónica previstos en los apartados a) y b) del artículo 13.2 de la Ley 11/2007 de 22 de junio. Estos sistemas de firma electrónica basada en certificados, requieren, sin embargo, actualizaciones de software y reconfiguraciones frecuentes que añaden un componente de complejidad que puede resultar disuasorio y que no es siempre necesario, en virtud del principio de proporcionalidad, en aquellos trámites y procedimientos que no requieran tan alto nivel de seguridad.

Por otra parte, aunque existen ya diferentes sistemas de identificación, autenticación y firma de los previstos en el artículo 13.2.c) de la Ley 11/2007, que prevé otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen, estos sistemas no son interoperables entre sí, con el trastorno que ello supone para el ciudadano al tener que conocer y aplicar distintos sistemas según la Administración, el organismo o el servicio o trámite al que acceda.

A la vista de estas dificultades, y en ejercicio de las funciones previstas en el artículo 9.1, apartado d) del Real Decreto 199/2012, de 23 de enero, que consisten en planificar la consolidación de las infraestructuras y servicios horizontales en el ámbito de la administración electrónica, el Ministerio de la Presidencia a través de la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado ha organizado y liderado los trabajos de un grupo de expertos en el que ha

participado representantes de la gran mayoría de los departamentos ministeriales y de sus organismos públicos adscritos, los cuales, tras un intenso trabajo de varios meses, han diseñado un sistema colaborativo de identificación, autenticación y firma electrónica, llamado a resolver las limitaciones de los actuales, integrando los sistemas de claves concertadas de la Administración ya existentes en uno único, y abriendo su utilización a la totalidad del Sector Público Administrativo Estatal, y permitiendo también integrarse al resto de las Administraciones Públicas cuando esté disponible, habilitando de este modo la extensión práctica de los servicios de Administración Electrónica a la gran mayoría de los ciudadanos españoles, en aplicación de la Ley 11/2007, de 22 de junio.

Por ello, atendiendo a las necesidades de los ciudadanos, aprovechando las posibilidades que la rápida evolución tecnológica ofrece y apelando al principio de proporcionalidad previsto en la Ley 11/2007, de 22 de junio, y sin perjuicio de la continuidad del servicio de los sistemas ya operativos, que resultan de indudable utilidad para los ciudadanos, se aprueba la creación de Cl@ve, un sistema común, de uso sencillo, basado en el artículo 13.2.c) de la citada ley que se conformará como la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas y ofrecerá servicios de identificación y autenticación alternativos y complementarios a los que se rigen por las letras a) y b) del artículo 13.2 de la Ley 11/2007, de 22 de junio. Este nuevo sistema pretende facilitar el acceso de los ciudadanos de forma uniforme a diversos servicios prestados vía Internet, tratando de minimizar los sistemas de identificación y autenticación existentes o aquellos que necesidades futuras pudieran demandar.

El sistema Cl@ve se desarrollará sobre dos sistemas ya operativos y, aprovechando el esfuerzo realizado en el seno del grupo de trabajo, se extiende el uso del PIN24H de la Agencia Estatal de Administración Tributaria, concebido para usuarios con acceso ocasional, y del «sistema de usuario y contraseña de la Seguridad Social» orientado a usuarios con acceso frecuente, recientemente implantados en sus respectivos ámbitos. Además, la transversalidad del nuevo modelo de gestión común de la identificación, autenticación y firma de los ciudadanos, al que se refiere el presente acuerdo, se fundamenta en la colaboración de los distintos órganos y organismos públicos adscritos a diversos departamentos ministeriales que actuarán en el sistema como órganos responsables de su aplicación y garantías de funcionamiento. Así, bajo la titularidad de la Dirección de Tecnologías de la Información y las Comunicaciones, que incorpora a las suyas las funciones hasta ahora atribuidas a la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, asumirán la responsabilidad de sus respectivas actuaciones en los ámbitos de Registro de usuarios, Identificación, Autenticación y Firma Electrónica la Agencia Estatal de Administración Tributaria, la Gerencia de Informática de la Seguridad Social y demás entidades Gestoras y Servicios Comunes de la Seguridad Social, la Dirección General de la Policía, como prestador de servicios de certificación, y a la FNMT-RCM, por la trascendencia que, en el desarrollo del proyecto, tiene el DNIe y la que en un futuro tendrá, sin duda, el DNI en la nube, ya que, adicionalmente, el sistema Cl@ve permitirá el acceso a servicios de firma en la nube basados en certificados electrónicos centralizados.

Este sistema de identificación y firma electrónica podrá evolucionar en el futuro para admitir también la participación del sector privado en su provisión, o su combinación con otras soluciones tecnológicas ofrecidas por empresas especializadas.

El sistema Cl@ve se crea para abarcar todo el ámbito del Sector Público Administrativo Estatal y, en su caso, del resto de las Administraciones Públicas. En este sentido cabe recordar que el impulso de una administración electrónica supone también dar respuesta a los compromisos comunitarios. La Agenda Digital para Europa propone medidas legales para el efectivo desarrollo digital de Europa en relación con la firma electrónica (acción clave n.º 3) y el reconocimiento mutuo de la identificación y la autenticación electrónicas (acción clave n.º 16), estableciendo así un marco jurídico claro con el fin de eliminar la fragmentación y la ausencia de interoperabilidad, potenciar la ciudadanía digital y prevenir la ciberdelincuencia.

En su desarrollo, la Ley 11/2007, de 22 de junio, consagra en su exposición de motivos el derecho de los ciudadanos a comunicarse con las Administraciones por medios electrónicos

e incide en que la contrapartida de este derecho es la obligación de las Administraciones de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse de forma ágil y eficaz. La administración electrónica no es asunto meramente técnico, sino de gobernanza democrática y la extensión de una plataforma común a todas las instancias administrativas viene a satisfacer esa necesidad de homogeneidad, sencillez y servicios compartidos que recoge el informe CORA.

Siendo el ámbito de aplicación de este texto el conjunto del Sector Público Administrativo Estatal, y formando parte del mismo la Administración General del Estado, se adopta este Acuerdo de Consejo de Ministros en virtud de lo dispuesto en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, en su artículo 11 «Otros sistemas de firma electrónica»; dictado en desarrollo del artículo 13.2.c) de la Ley 11/2007, que indica que cuando el sistema se refiera a la totalidad de la Administración General del Estado, se requerirá acuerdo del Consejo de Ministros a propuesta de los Ministerios de la Presidencia y de Industria, Turismo y Comercio, previo informe del Consejo Superior de Administración Electrónica.

En virtud de lo expuesto, previo informe del Consejo Superior de Administración Electrónica y a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia, del Ministro de Hacienda y Administraciones Públicas, del Ministro del Interior, de la Ministra de Empleo y Seguridad Social y del Ministro de Industria, Energía y Turismo, el Consejo de Ministros en su reunión de 19 de septiembre de 2014, acuerda:

Primero. *Aprobación del sistema Cl@ve.*

Se aprueba el sistema Cl@ve, un sistema de identificación, autenticación y firma electrónica común para todo el Sector Público Administrativo Estatal, que permitirá al ciudadano relacionarse electrónicamente con los servicios públicos a través de una plataforma común mediante la utilización de claves concertadas previo registro como usuario de la misma, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Esta plataforma ofrecerá a los usuarios una interfaz amigable para seleccionar alguno de los sistemas de identificación y firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio.

La información relativa a este sistema, así como la relación de organismos del Sector Público Estatal, Administraciones Autonómicas o Entidades Locales que se incorporen al sistema, será publicada en el Portal www.060.gob.es y en las sedes electrónicas de los organismos en los que sea de aplicación de acuerdo con lo previsto en el Real Decreto 1671/2009, de 6 de noviembre por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio.

Segundo. *Órganos responsables de su aplicación y garantías de funcionamiento.*

1. El órgano responsable del sistema Cl@ve será la Dirección de Tecnologías de la Información y las Comunicaciones, en desarrollo de las competencias para el impulso de la Administración digital, y del proceso de innovación de la Administración General del Estado y sus Organismos Públicos. atribuidas de acuerdo con lo dispuesto en el Real Decreto 802/2014, de 19 de septiembre, por el que se modifican el Real Decreto 390/1998, de 13 de marzo, por el que se regulan las funciones y la estructura orgánica de las Delegaciones de Economía y Hacienda; el Real Decreto 1887/2011, de 30 de diciembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales; el Real Decreto 199/2012, de 23 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia; el Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas y el Real Decreto 696/2013, de 20 de septiembre, de modificación del anterior.

2. Participarán en la construcción e implantación del sistema Cl@ve y serán garantes de su funcionamiento, los siguientes órganos y organismos públicos, que asumirán la responsabilidad de sus respectivas actuaciones en los ámbitos de Registro de usuarios, Identificación, Autenticación y Firma Electrónica:

a) La Agencia Estatal de Administración Tributaria.

b) La Dirección de Tecnologías de la Información y las Comunicaciones.

c) La Gerencia de Informática de la Seguridad Social y demás entidades Gestoras y Servicios Comunes de la Seguridad Social

d) La Dirección General de la Policía

e) La Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM).

3. A los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado tendrá la condición de responsable del fichero, siendo los órganos y organismos públicos mencionados en el párrafo anterior encargados del tratamiento de la mismo, de acuerdo con su normativa específica. Por ello, y de conformidad con lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, dichos órganos y organismos públicos:

a) Tratarán los datos necesarios para el funcionamiento del sistema por cuenta del órgano responsable del fichero y conforme a las indicaciones que el mismo establezca, conforme al apartado quinto de este Acuerdo.

b) No tratarán los datos para fines distintos de los propios del sistema que consisten en facilitar al ciudadano una plataforma común que le permita relacionarse electrónicamente con los servicios públicos mediante la utilización de claves concertadas.

c) Implantarán, para el adecuado funcionamiento del sistema, las medidas de seguridad establecidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

d) Deberán, en caso, de cesar en la prestación del servicio, proceder a la devolución de los datos o a su transmisión al órgano u organismo que a tal efecto designase el responsable del fichero.

e) Respetarán, lo establecido en el artículo 12 de la Ley Orgánica 15/1999 y en el Capítulo III del Título II de su Reglamento de desarrollo.

4. El sistema permitirá varios modos de utilización, con diferentes niveles de garantía de funcionamiento con arreglo a criterios de integridad, confidencialidad, autenticidad y no repudio, en los términos previstos en el art. 11.3 del Real Decreto 1671/2009, de 6 de noviembre, que podrán ser aplicados a los procedimientos administrativos en función de sus necesidades, en virtud del principio de proporcionalidad recogido en el artículo 4 de la Ley 11/2007, de 22 de junio.

Tercero. *Descripción general del sistema Cl@ve.*

1. Registro:

Los interesados que deseen utilizar el sistema deberán facilitar los datos de carácter personal necesarios para habilitar los servicios de identificación, autenticación y firma electrónicas. Estos datos se integrarán en el Fichero Cl@ve de datos de carácter personal que se creará en los términos previstos en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

El registro podrá realizarse de forma telemática o presencial en cualquiera de las oficinas de los órganos y organismos públicos que realicen funciones de Registro de usuarios de la plataforma Cl@ve. La forma de registro utilizada será uno de los factores para clasificar el nivel de garantía de identidad y autenticidad asociado al registro.

2. Identificación:

Existirán 2 tipos de sistemas de identificación:

a) Cl@ve ocasional: sistema de contraseña de validez muy limitada en el tiempo, orientado a usuarios que acceden esporádicamente a los servicios.

b) Cl@ve permanente: sistema de contraseña de validez duradera en el tiempo pero no ilimitada, orientado a usuarios habituales.

3. Firma de documentos electrónicos:

Los sistemas de Cl@ve podrán utilizarse para confirmar información, propuestas o borradores remitidos o exhibidos por una Administración Pública.

La plataforma Cl@ve ofrecerá a los usuarios una interfaz amigable que les permita seleccionar, de entre los sistemas de firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio, aquellos que exija o permita en cada caso la normativa reguladora de la actuación de que se trate para realizar el trámite o gestión administrativa correspondiente y la firma de documentos electrónicos en su caso.

Entre los sistemas ofrecidos al ciudadano, la plataforma Cl@ve ofrecerá al ciudadano utilizar el Documento Nacional de Identidad Electrónico para su identificación, autenticación y firma, en cuyo caso será aplicable al tratamiento de datos derivado de dicha utilización la normativa reguladora del citado documento.

Cuarto. *Aplicación del sistema.*

1. Cuando la realización de trámites o el acceso a servicios en una Sede Electrónica del Sector Público Administrativo Estatal requiera el uso de sistemas de identificación y autenticación de los previstos en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberá ofrecerse, como mínimo, alguno de los sistemas que se integren en la nueva plataforma Cl@ve.

2. Asimismo, con el fin de facilitar el acceso electrónico de los ciudadanos a la Administración y en desarrollo del principio de eficiencia, podrán adherirse al sistema mediante convenio otras Administraciones Públicas en las condiciones técnicas, económicas y organizativas que se determinen en las prescripciones técnicas de desarrollo a las que se refiere el apartado Quinto de este Acuerdo. Su incorporación al sistema Cl@ve será publicada en el Portal www.060.gob.es y en las sedes electrónicas que sean de aplicación.

3. Inicialmente funcionarán como Oficinas de Registro de datos la red de oficinas de la Agencia Estatal de Administración Tributaria y de las Entidades Gestoras y Servicios Comunes de la Seguridad Social. La Dirección de Tecnologías de la Información y las Comunicaciones de la Administración General del Estado podrá acordar ampliar la red de Oficinas de Registro con aquellos organismos públicos que dispongan de despliegue territorial y cumplan los requisitos técnicos necesarios establecidos por resolución de esta Dirección. La relación de Oficinas de Registro será publicada en el Portal www.060.gob.es y en las sedes electrónicas que sean de aplicación.

4. El Sector Público Administrativo Estatal deberá habilitar el sistema Cl@ve en todos los servicios y trámites electrónicos dirigidos a los ciudadanos antes del 31 de diciembre de 2015. Estarán excluidos los servicios y trámites dirigidos a ciudadanos que estén obligados por la normativa vigente al uso exclusivo de certificados electrónicos incluidos en el ámbito de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica, así como el resto de trámites o servicios en los que la normativa reguladora no permita la utilización por los ciudadanos de los sistemas de identificación, autenticación y firma contemplados en la letra c) del artículo 13.2 de la Ley 11/2007, de 22 de junio.

Quinto. *Prescripciones técnicas.*

La Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado establecerá, mediante resolución, las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, incluidos los siguientes aspectos:

1. Los elementos tecnológicos, procedimentales y organizativos necesarios para el desarrollo e implementación del sistema, y el aseguramiento de cada uno de los niveles de garantía de funcionamiento asociados a cada sistema de identificación de los previstos en este acuerdo.

2. Los procedimientos de registro de nuevos usuarios y los procedimientos para la incorporación de usuarios existentes en otros sistemas de firma ya operativos de los contemplados en el artículo 13.2 c) de la Ley 11/2007, de 22 de junio, previo consentimiento expreso de los mismos en los términos establecidos en la Ley 15/1999, de 13 de diciembre.

3. Las condiciones técnicas, económicas y organizativas para la incorporación de otras Administraciones Públicas al sistema Cl@ve.

4. El sistema de identificación e imputación de costes de mantenimiento y explotación del sistema Cl@ve correspondientes a órganos y organismos del Sector Publico Administrativo Estatal.

5. En general, todas las cuestiones necesarias para asegurar el funcionamiento de Cl@ve y su interoperabilidad.

Sexto. *No incremento del gasto público.*

La aplicación de las medidas previstas en el presente acuerdo se llevará a cabo sin incremento de gasto público.

Séptimo. *Efectos.*

El presente Acuerdo se publicará en el «Boletín Oficial del Estado», en el Portal www.060.gob.es y en las sedes electrónicas de los órganos y organismos de aplicación y producirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 16

Resolución de 14 de julio de 2017, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica, en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos

Ministerio de Hacienda y Función Pública
«BOE» núm. 170, de 18 de julio de 2017
Última modificación: 21 de octubre de 2022
Referencia: BOE-A-2017-8393

El artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, enumera los sistemas válidos a efectos de firma, que los interesados podrán utilizar para relacionarse con las Administraciones Públicas.

El citado precepto se refiere expresamente a los sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica, a los sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello electrónico y a cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan, recogiendo asimismo la posibilidad de admitir los sistemas de identificación contemplados en la Ley como sistemas de firma.

En cualquier caso, todos los sistemas de firma electrónica admitidos deberán garantizar el cumplimiento de los requisitos recogidos en el apartado primero del artículo 10 de la citada Ley. Esto es, que estos sistemas permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, así como la integridad e inalterabilidad del documento.

A estos sistemas de firma electrónica han de reconocérsele efectos jurídicos y son conformes a lo establecido en el artículo 25.1 del Reglamento (UE) N o 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, sin menoscabo de lo recogido en el artículo 27 de la propia norma «Firmas electrónicas en servicios públicos».

El artículo 11 de la Ley 39/2015, de 1 de octubre regula el uso de los medios de identificación y firma en el procedimiento administrativo estableciendo que, con carácter general, para realizar cualquier actuación prevista en el procedimiento administrativo sólo será necesario identificarse, y limitando la obligatoriedad de la firma para los supuestos previstos en el apartado segundo del artículo: Formular solicitudes, presentar declaraciones

responsables o comunicaciones, interponer recursos, desistir de acciones y renunciar a derechos. Esta importante novedad en la regulación aconseja establecer las cautelas mínimas que permitan normalizar el uso de estos sistemas evitando la heterogeneidad de su implementación técnica entre las Administraciones.

Así, y en aplicación de lo dispuesto en el artículo 10.3 de la Ley 39/2015, de 1 de octubre, que faculta a las Administraciones Públicas a admitir los sistemas de identificación contemplados en esta Ley como sistema de firma cuando permitan acreditar la autenticidad de la expresión de la voluntad y consentimiento de los interesados, siempre que así lo disponga la normativa reguladora, se procede con esta resolución a indicar los requisitos que se tienen que cumplir, no sólo con este objetivo, sino para asegurar también la integridad e inalterabilidad de los datos firmados, así como los requisitos para comprobar que se realizó dicho acto. Por lo tanto, se sientan las bases de uso de sistemas de identificación basados en la plataforma Cl@ve, para la realización de la firma, así como se establece una recomendación para recoger las evidencias de actos de relevancia jurídica, como las notificaciones, que si bien no necesitan firma, sí pueden necesitar unos requisitos de seguridad reforzados, manteniendo siempre el espíritu de la ley por el que no se haga en ningún caso más complejo para el ciudadano la recepción de la notificación o la realización de un trámite.

Es importante subrayar además, la complementariedad de esta resolución con el proyecto Cl@ve firma, que provee sencillos mecanismos para facilitar la firma electrónica criptográfica, de manera que se evitan los principales problemas, como la necesidad de disponer de hardware y/o software específico para realizar la firma en el ordenador del interesado, ya que toda esa complejidad queda resuelta por el sistema Cl@ve firma. Si bien este sistema es óptimo desde el punto de vista de uso de firma criptográfica, requiere que el ciudadano tenga activa la identificación por Cl@ve Permanente que le permite acceder a su certificado electrónico centralizado, en el caso de no tener activa esta identificación y siempre que el servicio lo permita esta nueva forma de firma no basada en certificado electrónico es una facilidad más para el ciudadano.

Por ello se ha tenido a bien el complementar este sistema de firma criptográfica sencilla para el ciudadano, con un sistema de medidas de seguridad, trazabilidad e integridad suficientes para los procedimientos que hagan uso de él, pero sin necesidad de recordar o tener activa una contraseña ni un certificado electrónico centralizado.

También resulta apropiado el uso de este sistema cuando, aun habiéndose utilizado un certificado electrónico en el proceso de identificación, no se quiera realizar una firma electrónica local con dicho certificado, para evitar los problemas de restricciones de compatibilidad de navegadores, máquinas virtuales Java y versiones de sistemas operativos.

Por tanto, el objeto de esta Resolución es establecer los criterios de uso y las condiciones técnicas de implementación de los sistemas de firma electrónica no criptográfica, previstos en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre, que se considerarán válidos a efectos de firma en la Administración General del Estado y sus organismos públicos, así como en aquellas otras Administraciones Públicas que adopten estos criterios y condiciones técnicas.

En virtud de lo anterior, y de acuerdo con el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los Departamentos ministeriales,

Esta Secretaría General de Administración Digital, en el ejercicio de las competencias atribuidas para la definición de estándares, de directrices técnicas y de gobierno TIC, de normas de seguridad y calidad tecnológicas y de la información a los que deberán ajustarse todas las Unidades de la Administración General del Estado y sus organismos públicos, dispone:

Primero.

1. Aprobar los términos y condiciones de uso de firma electrónica no criptográfica en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos, de acuerdo con el artículo 10.2 de la Ley 39/2015, de 1 de octubre, que se incluyen como anexo.

2. Ordenar su publicación en el «Boletín Oficial del Estado».

Segundo.

La presente Resolución entra en vigor a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

ANEXO

Términos y condiciones de uso de la firma electrónica no criptográfica en las relaciones de los interesados con los órganos administrativos de la Administración General del Estado y sus organismos públicos

I. Objeto

Los presentes términos y condiciones tienen como objeto determinar las circunstancias en las que un sistema de firma electrónica no basado en certificados electrónicos será considerado como válido en las relaciones de los interesados con los órganos de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes, de acuerdo con lo previsto en el artículo 10.2.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas Sin perjuicio, de otros sistemas de firma implantados, de acuerdo con el artículo 10.2.c) y 10.4 y que ofrezcan las garantías de seguridad suficientes para gestionar la integridad y el no repudio, según el principio de proporcionalidad previsto en el artículo 14.3 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

II. Ámbito de aplicación

Los presentes términos y condiciones serán de aplicación a los órganos administrativos de la Administración General del Estado y organismos públicos y entidades de Derecho Público vinculados o dependientes, que habiliten nuevos sistemas de firma electrónica no criptográfica destinados a ser usados por los interesados en sus relaciones con los mismos, y sin perjuicio de la posibilidad de utilización en tales trámites de los sistemas de firma contemplados en el artículo 10.2.a) de la Ley 39/2015, de 1 de octubre.

III. Criterios para la utilización de sistemas de firma electrónica no criptográfica

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, constituye el marco normativo que permite definir y establecer las medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los interesados y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En la implantación de un sistema de firma electrónica no criptográfica se cumplirá con el Esquema Nacional de Seguridad para garantizar la seguridad de los datos y los servicios, como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

En aplicación de esta norma, se podrán utilizar sistemas de firma electrónica no criptográfica cuando el sistema de información asociado al procedimiento haya sido categorizado, según el esquema nacional de seguridad, de categoría básica y aquellos de categoría media en los que no sea necesario utilizar la firma electrónica avanzada, cuando así lo disponga la normativa reguladora aplicable.

IV. Garantía de funcionamiento

Cuando la actuación realizada por el interesado, en su relación con la Administración, implique la presentación en una sede electrónica de documentos electrónicos utilizando los sistemas de firma electrónica contemplados en la presente Resolución, se garantizará la integridad de la información presentada mediante el sellado realizado con el sello electrónico cualificado o reconocido del organismo competente para la gestión del procedimiento, a la que se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un

prestador de sellado de tiempo supervisado, y su incorporación inmediata al sistema de información asociado a dicho procedimiento. El organismo deberá disponer de las medidas técnicas, organizativas y procedimentales necesarias para garantizar dicha integridad a lo largo del tiempo.

Asimismo, se garantizará también la integridad, mediante el sellado realizado con el sello electrónico cualificado o reconocido del organismo y la adición de un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, de las evidencias necesarias para la verificación de la identidad, recopiladas inmediatamente antes del acto de la firma, así como, posteriormente, del consentimiento explícito del interesado con el contenido firmado, almacenando dichas evidencias en el sistema de información junto con la información presentada. La integridad y conservación de los documentos electrónicos almacenados y de sus metadatos asociados obligatorios quedará garantizada a través del sellado con el sello electrónico cualificado o reconocido del organismo y del resto de medidas técnicas que aseguren su inalterabilidad.

El organismo responsable del procedimiento emitirá un justificante de firma sellado con su sello electrónico de órgano y generando el código seguro de verificación o CSV, que será el documento con valor probatorio de la actuación realizada. La integridad de los documentos electrónicos autenticados mediante CSV podrá comprobarse mediante el acceso directo y gratuito a la sede electrónica del organismo y en el punto de acceso general de la Administración General del Estado, en tanto no se acuerde la destrucción de dichos documentos con arreglo a la normativa que resulte de aplicación o por decisión judicial.

V. Acreditación de la autenticidad de la expresión de la voluntad y consentimiento del interesado

Para acreditar la autenticidad de la expresión de la voluntad y consentimiento del interesado se requerirá:

1. La autenticación del interesado, inmediatamente previa a la firma utilizando la plataforma Cl@ve, de identificación electrónica.
2. La verificación previa por parte del interesado de los datos a firmar.

Estos datos se obtendrán a partir de aquella información presentada por el ciudadano y de cuya veracidad se hace responsable, así como de los documentos electrónicos que, eventualmente, presente en el procedimiento.

3. La acción explícita por parte del interesado de manifestación de consentimiento y expresión de su voluntad de firma.

V.1. Autenticación del interesado. La identificación y autenticación del interesado deberá hacerse, en todo caso, a través de la plataforma Cl@ve, sistema de identificación, autenticación y firma electrónica basado en claves concertadas, común para todo el sector público administrativo estatal, aprobado por Acuerdo de Consejo de Ministros de 19 de septiembre de 2014.

Dicha autenticación del interesado con el sistema Cl@ve deberá ser inmediatamente previa al acto de firma.

V.2. Verificación previa de los datos a firmar. El interesado debe ser consciente de los datos que va a firmar y deberá ofrecérsele de un modo visible la posibilidad de consultarlo en un formato legible y, preferiblemente, con el mismo formato del documento que posteriormente se entregue al interesado como justificante de la firma.

V.3. Expresión del consentimiento y de la voluntad de firma de los interesados. Las aplicaciones que hagan uso de un sistema de firma, ajustado a los criterios de uso y condiciones técnicas de esta Resolución, deberán requerir de forma expresa la expresión del consentimiento y la voluntad de firma del interesado en el procedimiento, mediante la inclusión de frases que pongan aquéllos de manifiesto de manera inequívoca, y la exigencia de acciones explícitas de aceptación por parte del interesado (por ejemplo, mediante una casilla junto al texto «Declaro que son ciertos los datos a firmar/muestro mi conformidad con el contenido del documento y confirmo mi voluntad de firmar» que el interesado debe marcar, y un botón «Firmar y enviar» que debe pulsar para realizar la firma).

VI. Garantía de no repudio

VI.1. Garantías en el proceso de firma. Para garantizar el no repudio de la firma por parte del interesado firmante, el sistema de firma deberá acreditar la vinculación de la expresión de la voluntad y los datos firmados con la misma persona. Para ello se volverá a solicitar la autenticación del interesado en el momento de proceder a la firma.

Asimismo, la garantía de no repudio exige que el sistema de firma asegure una adecuada trazabilidad en el caso de que sea necesario auditar una operación de firma concreta, para lo cual conservará, por cada firma y, por tanto, por cada proceso de autenticación, la siguiente información:

a) Fecha y hora de la autenticación.

b) Nombre y apellidos del interesado.

c) DNI/NIF/NIE del interesado.

d) Sistema de identificación empleado (certificado electrónico, Cl@ve PIN o Cl@ve Permanente) y nivel de seguridad de identificación.

e) Resultado exitoso de la autenticación.

f) Respuesta devuelta y firmada por la plataforma Cl@ve. Esta respuesta deberá incluir el campo opcional que contiene la respuesta devuelta y firmada por el Proveedor de servicios de Identificación.

g) Fecha y hora de la firma.

h) Resumen criptográfico de los datos firmados, con un algoritmo de hash que cumpla las especificaciones del esquema nacional de seguridad.

i) Referencia al justificante de firma, mediante el CSV asociado a dicho justificante.

La información a que se refieren los párrafos anteriores será sellada con un certificado de sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo. Adicionalmente, se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y será almacenada, como evidencia de la verificación de la identidad previa al acto de la firma, vinculada a los datos firmados.

En el caso de que los datos de identificación obtenidos en la autenticación inmediatamente anterior a la firma no coincidan con los datos de identificación obtenidos en autenticaciones previas, el sistema de firma no permitirá la realización de la misma, informando de esa eventualidad al sistema de información asociado al procedimiento o servicio electrónico que requiere dicha firma.

VI.2. Gestión de las evidencias de autenticación. A pesar de que el sistema de firma proporcionará a los sistemas de información asociados al procedimiento electrónico que requiere la firma la información relativa a la autenticación vinculada a dicha firma, en ocasiones puede ser necesario, por motivos de auditoría, recuperar las evidencias completas del proceso de autenticación.

Al utilizar el sistema Cl@ve como mecanismo de identificación y autenticación, las evidencias últimas no residen en el propio sistema de firma, sino en los sistemas de los proveedores de servicios de identificación integrados en Cl@ve.

Con objeto de que los proveedores de esos servicios de identificación puedan recuperar las evidencias necesarias para acreditar la realización de la identificación y autenticación previas ligadas a la realización de una firma en el sistema, se deberá facilitar a dichos proveedores la información de autenticación almacenada como evidencia de la verificación previa de la identidad en los sistemas de información asociados al procedimiento administrativo que requiere la firma, descrita en el apartado VI.1.

A tal efecto, los proveedores de servicios de identificación deberán salvaguardar dichas evidencias durante el plazo mínimo de cinco años. La solicitud de certificación de dichas evidencias se realizará conforme al procedimiento y las condiciones que se publicarán en el portal de Administración electrónica.

VII. Garantía de la integridad de los datos y documentos firmados

VII.1. Sellado de la información presentada. Una vez acreditada la expresión de la voluntad y el consentimiento y para firmar del interesado, se deberán establecer los mecanismos para garantizar la integridad e inalterabilidad de los datos y, en su caso, de los documentos electrónicos presentados por el interesado, para lo cual el sistema de firma sellará los datos a firmar, con un sello de órgano y la adición de un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y la pondrá a disposición del sistema de información asociado al procedimiento electrónico que requiere la firma.

VII.2. Justificante de firma. En el proceso de firma se entregará al interesado un justificante de firma, que será un documento legible, de acuerdo con la norma técnica de interoperabilidad de catálogo de estándares y preferiblemente en formato PDF y que deberá cumplir estos requisitos:

– Garantizar la autenticidad del organismo emisor mediante un sellado electrónico con el certificado de sello del mismo, en formato PAdES en el caso de que el justificante tenga el formato PDF.

– Contener los datos del firmante y, en el caso de que el documento firmado haya pasado por un Registro de entrada, los datos identificativos de su inscripción en el Registro.

– Contener los datos a firmar expresamente por el interesado. Si se ha anexado algún documento electrónico se incluirá una referencia al mismo.

– Garantizar el instante en que se realizó la firma, mediante sello de tiempo del justificante, realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado.

– Garantizar la autenticidad del justificante de firma, incluyendo en el justificante de firma un código seguro de verificación (CSV), y garantizando que este justificante se pueda consultar en línea mediante un sistema de cotejo de CSV cuya dirección se incluya en el propio justificante de firma.

– Alternativamente, la autenticidad del organismo emisor y del justificante de firma se podrá garantizar mediante dos documentos: uno de ellos con sellado electrónico del justificante en formato PAdES (en el caso de que el justificante tenga formato PDF) y otro con la utilización de un código seguro de verificación (CSV) del justificante.

§ 17

Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 311, de 29 de diciembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-14215

El Consejo de Ministros, en su reunión de 19 de septiembre de 2014 y, a propuesta de la Vicepresidenta del Gobierno y Ministra de la Presidencia y de los Ministros de Hacienda y Administraciones Públicas, del Interior, de Empleo y Seguridad Social y, de Industria, Energía y Turismo adoptó un Acuerdo por el que se aprueba Cl@ve, un sistema de identificación, autenticación y firma electrónica común para todo el Sector Público Administrativo Estatal que permitirá al ciudadano relacionarse electrónicamente con los servicios públicos a través de una plataforma común, mediante la utilización de claves concertadas previo registro como usuario de la misma, conforme a lo previsto en el artículo 13.2c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El citado Acuerdo publicado por Orden PRE/1838/2014, de 8 de octubre, determina en su apartado quinto, «Prescripciones Técnicas», que corresponde a la Dirección de Tecnologías de la Información y de las Comunicaciones de la Administración General del Estado, establecer mediante resolución, las Prescripciones Técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, y determina los aspectos que dichas prescripciones deben incluir.

En virtud de lo anterior, esta Dirección de Tecnologías de la Información y de las Comunicaciones resuelve:

Primero.

1. Aprobar las Prescripciones Técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve, en los términos recogidos en el Acuerdo de Consejo de Ministros de fecha de 19 de septiembre de 2014, por el que se aprueba Cl@ve, la plataforma común del Sector Público Administrativo Estatal para la identificación, autenticación y firma electrónica mediante el uso de claves concertadas, que se incluyen como anexo.
2. Ordenar su publicación en el «Boletín Oficial del Estado».

Segundo.

La presente Resolución entra en vigor a partir del día siguiente a su publicación en el «Boletín Oficial del Estado».

PRESCRIPCIONES TÉCNICAS NECESARIAS PARA EL DESARROLLO Y APLICACIÓN DEL SISTEMA CL@VE

I. Objeto

Las presentes Prescripciones Técnicas tienen por objeto establecer los aspectos necesarios para el desarrollo y aplicación del sistema Cl@ve, así como para asegurar su funcionamiento e interoperabilidad.

II. Ámbito de aplicación

Las presentes Prescripciones Técnicas serán de aplicación a:

a) Los órganos y organismos públicos participantes en la construcción e implantación del sistema Cl@ve y garantes de su funcionamiento.

b) Los órganos y organismos públicos del Sector Público Administrativo Estatal obligados a habilitar el sistema Cl@ve en todos los servicios y trámites electrónicos dirigidos a los ciudadanos.

c) Otras Administraciones Públicas que se adhieran al sistema.

d) Las entidades del sector privado que participen en el futuro como proveedores de sistemas de identificación y firma electrónica integrados con Cl@ve.

III. Propósito del sistema Cl@ve

Cl@ve es un sistema de Identificación, Autenticación y Firma Electrónica común para todo el Sector Público Administrativo Estatal, basado en el uso de claves concertadas, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El sistema Cl@ve está dirigido a ciudadanos españoles y extranjeros que cumplan los requisitos indicados en estas Prescripciones Técnicas y proporciona dos modalidades diferenciadas de identificación y autenticación basadas en el uso de claves concertadas para el acceso de los ciudadanos a los servicios electrónicos que hagan uso de este sistema, complementando los actuales sistemas de acceso mediante DNI-e y certificado electrónico reconocido.

Con este propósito, el sistema Cl@ve ofrecerá una interfaz amigable que permita al usuario seleccionar alguno de los sistemas de identificación y firma electrónica señalados en el artículo 13.2 de la Ley 11/2007, de 22 de junio.

Asimismo, el sistema Cl@ve permitirá al ciudadano el acceso al servicio de firma de documentos por medio de certificados electrónicos albergados tanto en modo local (por ejemplo en su PC) o en dispositivos conectados al mismo (por ejemplo, en el DNI-e) como en modo centralizado.

IV. Niveles de garantía, sistemas de identificación, y firma de documentos electrónicos

IV.1 Registro de usuarios.

Con objeto de garantizar un nivel adecuado de calidad en la identificación y autenticación que se llevan a cabo mediante el sistema Cl@ve, la utilización de dicho sistema requiere de un registro previo de los usuarios. Mediante dicho registro, se verifica la existencia de una persona física real asociada a la identidad electrónica que utilizará el sistema, se obtienen un conjunto de datos personales asociados a esa identidad, y se obtiene el consentimiento del usuario para que dichos datos personales sean incorporados al fichero de datos personales del sistema y sean tratados para la finalidad con la que se ha desarrollado el mismo.

Se podrán registrar en Cl@ve ciudadanos españoles con Documento Nacional de Identidad (DNI) y ciudadanos extranjeros con Tarjeta de Identidad de Extranjeros (TIE) o Certificado de Ciudadano de la Unión Europea; en ambos casos los documentos habrán de estar en vigor. La posibilidad de registro podrá ser extendida a ciudadanos españoles residentes en el extranjero sin DNI en vigor, mediante la habilitación de procedimientos de verificación de la identidad equivalentes a los establecidos para los ciudadanos con DNI.

Existirán dos modalidades o niveles de garantía de registro asociados a la forma y a las garantías que ofrezca la comunicación de la información de registro por parte del ciudadano:

a) Nivel Básico, en el que los datos del registro de usuario son facilitados por el ciudadano de forma telemática, pero sin una autenticación previa mediante certificado electrónico reconocido. La identificación se realizará utilizando datos conocidos por el ciudadano y la administración.

b) Nivel Avanzado, en el que los datos del registro de usuario son facilitados por el ciudadano, bien de forma presencial en una oficina ante un empleado público habilitado al efecto, o bien, son comunicados de forma telemática, previa autenticación del ciudadano mediante un certificado electrónico reconocido.

El nivel de garantía asociado al procedimiento de registro empleado quedará almacenado en el sistema Cl@ve, y podrá ser utilizado para seleccionar los modos de identificación válidos para cada procedimiento, en aplicación del principio de proporcionalidad previsto en el artículo 4 de la Ley 11/2007, de 22 de junio.

IV.2 Modalidades de identificación.

El sistema Cl@ve proporcionará a los usuarios dos modalidades de identificación electrónica basadas en el uso de claves concertadas, cada una de las cuales proporcionará dos niveles distintos de garantía en la autenticación:

c) Cl@ve ocasional o Cl@ve PIN: Modalidad de identificación para el acceso al sistema en el cual la contraseña, limitada a un solo uso, está formada por una clave aportada por el usuario más un código que recibe en su dispositivo móvil y que tiene una validez muy limitada en el tiempo. Está orientado a usuarios que acceden esporádicamente a los servicios.

El sistema de acceso basado en Cl@ve ocasional podrá ser denominado indistintamente Cl@ve PIN cuando sea mostrado a los usuarios del sistema para facilitar su identificación y acceso.

d) Cl@ve permanente: Modalidad de identificación para el acceso al sistema por medio de un identificador (Número de DNI o NIE del usuario) y una contraseña que debe ser custodiada por el ciudadano. La validez de la contraseña es duradera en el tiempo, pero no ilimitada. Adicionalmente, y cuando el tipo de trámite lo requiera, la modalidad de identificación Cl@ve permanente podrá proporcionar un nivel superior de garantía en la autenticación, para lo cual requerirá la utilización de una verificación de seguridad adicional mediante un código de un solo uso (OTP, «Once Time Password») y validez limitada en el tiempo enviado al dispositivo móvil del usuario. Está orientado principalmente para uso por parte de usuarios habituales.

Los requisitos de seguridad de las contraseñas para este sistema se publicarán en el portal Cl@ve (www.clave.gob.es)

El usuario podrá elegir en el momento de iniciar sesión en el Sistema Cl@ve qué modalidad de identificación prefiere utilizar, en función de las limitaciones establecidas por el proveedor de servicios electrónicos integrado con Cl@ve en cuanto a los niveles de garantía exigidos por el procedimiento o trámite al que se desea acceder.

IV.3 Firma de documentos electrónicos.

El sistema Cl@ve permitirá también el acceso a servicios de firma electrónica, en particular, a servicios de firma de documentos electrónicos mediante certificados electrónicos centralizados, todo ello a efecto de su presentación ante las Administraciones Públicas en aquellos trámites en que la firma mediante certificados electrónicos sea requerida o admitida. Se tendrán en cuenta las siguientes consideraciones:

a) Para poder acceder al servicio, el usuario deberá solicitar previa y expresamente la emisión de los certificados electrónicos centralizados correspondientes que posibilitan la firma mediante la plataforma Cl@ve.

b) Los certificados electrónicos centralizados serán emitidos con las mismas garantías de identificación del DNI electrónico del ciudadano

c) Para realizar la solicitud, y para el acceso ulterior al servicio, será necesario en todo caso que el usuario se haya registrado en Nivel Avanzado y haya activado su Cl@ve

permanente. Además se requerirá en el momento de la identificación la utilización de una verificación de seguridad adicional mediante un código de un solo uso y validez limitada en el tiempo que se enviará al teléfono móvil del usuario registrado.

A estos efectos, es de aplicación lo dispuesto en el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

IV.4 Punto de acceso al sistema Cl@ve.

Para facilitar el acceso a los servicios de identificación y autenticación del sistema Cl@ve, se creará un punto de acceso electrónico desde el que el ciudadano podrá identificarse de acuerdo a los diferentes niveles de garantía previstos en estas Prescripciones Técnicas. Con este propósito, el punto de acceso presentará un menú que permitirá al usuario elegir la modalidad de identificación electrónica deseada de entre las opciones puestas a disposición por el proveedor del servicio electrónico que soporta el tipo de trámite o procedimiento que desee realizar, de acuerdo con los niveles de garantía en el registro y la autenticación exigidos por dicho trámite o procedimiento.

El punto de acceso permitirá acceder a los servicios de identificación y autenticación previstos en el sistema Cl@ve, así como, en el futuro, a otros sistemas de identificación, entre ellos los sistemas de identificación electrónica de ámbito europeo admitidos en virtud de la normativa de la Unión Europea aplicable. Asimismo, el proveedor del servicio a efectos del cumplimiento del artículo 13 de la Ley 11/2007, podrá optar por habilitar sistemas de identificación no basados en claves concertadas complementarios al sistema Cl@ve, o por habilitar el acceso mediante el sistema Cl@ve a los medios de identificación previstos en el artículo 13.2, apartados a) y b) de la Ley 11/2007, opción que deberá incluir en todo caso los sistemas de firma electrónica incorporados al Documento Nacional de Identidad.

Las diversas Sedes Electrónicas de la Administración que requieran utilizar un sistema de identificación y autenticación de los previstos en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, deberán ofrecer, como mínimo, alguno de los sistemas de identificación mediante claves concertadas que se integren en la nueva plataforma Cl@ve.

Con este propósito, dichas Sedes Electrónicas deberán integrarse con el sistema Cl@ve actuando como proveedoras de servicios, redirigiendo automáticamente al ciudadano desde la sede electrónica al Punto de Acceso del sistema Cl@ve cuando el ciudadano desee realizar un trámite o procedimiento que precise algún sistema de identificación y autenticación de los previstos en el sistema Cl@ve. En esa redirección, las entidades deberán especificar el nivel de garantía en la autenticación que requiere el procedimiento o trámite al que desea acceder el ciudadano, pudiendo opcionalmente especificar también el nivel exigido de calidad en el registro. Una vez realizada la verificación de la identidad por parte de la entidad responsable de la modalidad de identificación seleccionada, el usuario será redirigido automáticamente al punto de origen, junto con el resultado de la autenticación, los datos que permiten identificar de manera no ambigua al ciudadano, y los niveles de garantías asociados a esa identidad.

Cuando el ciudadano se haya identificado y autenticado previamente en un servicio electrónico integrado con Cl@ve a través del Punto de Acceso, desde este Punto de Acceso se le dará la posibilidad de acceder a otro servicio electrónico sin necesidad de identificarse de nuevo, siempre que el proveedor de este segundo servicio lo permita. Esto supondrá que el ciudadano no tendrá que introducir los datos de identificación asociados a su Cl@ve PIN o Cl@ve Permanente.

Para asegurar esta integración con el Punto de Acceso del sistema Cl@ve, las entidades usuarias del sistema deberán seguir las especificaciones técnicas de integración definidas por las entidades responsables del mismo. Con el objeto de facilitar dicha integración, se habilitará un conjunto de componentes comunes, orientados a simplificar el manejo de los mensajes de petición y respuesta intercambiados durante el proceso de identificación y autenticación, que las entidades usuarias podrán incorporar a sus servicios electrónicos. Dichas especificaciones y componentes comunes se publicarán en el Centro de Transferencia de Tecnología.

La transmisión de información entre el Punto de Acceso del sistema Cl@ve y las sedes electrónicas integradas se protegerá de acuerdo con las mejores prácticas técnicas con

objeto de asegurar la privacidad, confidencialidad e integridad de dicha información. En este sentido, el Punto de Acceso del sistema Cl@ve no almacenará ningún dato de carácter personal, sino únicamente información técnica no vinculada a personas físicas o jurídicas, con el objeto de garantizar, en el caso de que se produzca un incidente, la reconstrucción, con la participación del proveedor del servicio electrónico al que accede el usuario y del proveedor del servicio de identificación de la modalidad de identificación escogida por este, de la secuencia de mensajes intercambiados entre los distintos actores del sistema para determinar el momento en que se produjo ese incidente y su naturaleza.

En el caso particular de los servicios electrónicos ofrecidos por los propios proveedores de servicios de verificación de la identidad de Cl@ve (AEAT y Seguridad Social, inicialmente), esta redirección al Punto de Acceso del sistema Cl@ve podrá ser sustituida por un acceso directo y equivalente a los servicios de verificación de la identidad de Cl@ve ofrecidos por dicho proveedor, siempre que el servicio electrónico no exija otro tipo de identificación diferente.

Adicionalmente, para facilitar el acceso a los servicios de firma electrónica con certificados electrónicos centralizados y presentar a los ciudadanos un mecanismo de firma uniforme en todo el sistema, se habilitará un conjunto de componentes de firma comunes que deberán ser integrados en las sedes electrónicas que requieran la realización de firma electrónica en sus trámites o procedimientos.

El Anexo I detalla los procedimientos de registro en el sistema Cl@ve, acceso al sistema Cl@ve y firma electrónica de documentos con certificados electrónicos centralizados asociados a los niveles de garantía del sistema Cl@ve previstos en estas Prescripciones Técnicas.

IV.5 Seguridad.

El sistema Cl@ve y todos los servicios asociados se implementarán garantizando su funcionamiento conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 11/2007, de 22 de junio, en el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010, de 8 de enero y conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y a su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

V. Entidades encargadas del sistema, funciones y garantías aportadas por cada una

V.1 Registro de usuarios.

La Agencia Estatal de Administración Tributaria (AEAT) actuará como organismo principal responsable del sistema de Registro de usuarios de Cl@ve.

A tales efectos, este organismo será responsable del funcionamiento de los sistemas de registro de usuarios descritos en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito del registro de usuarios.

Inicialmente, con el fin de ofrecer un mejor servicio a los ciudadanos, estarán habilitadas y dispondrán de los medios necesarios para realizar funciones de registro de usuarios del sistema Cl@ve, además de la red de oficinas de la AEAT, las entidades gestoras de la Seguridad Social.

La Dirección de Tecnologías de la Información y las Comunicaciones (DTIC) podrá acordar la adhesión al sistema de otros órganos y organismos del Sector Público Administrativo Estatal para actuar como oficina de registro de usuarios Cl@ve a fin de ofrecer a los ciudadanos nuevos puntos presenciales de registro, así como de órganos y organismos públicos pertenecientes a otras Administraciones.

En virtud de lo anterior, se ha habilitado para actuar como oficinas de registro presencial del sistema Cl@ve a la Red de oficinas de Información y Atención al Ciudadano de las Delegaciones y Subdelegaciones de Gobierno.

Los órganos y organismos distintos de la AEAT que actúen como oficinas de registro tendrán que cumplir los requisitos establecidos en la Resolución de 28 de septiembre de 2015 de la Dirección de Tecnologías de la Información y las Comunicaciones por la que se

establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

La DTIC mantendrá la relación de oficinas de registro de Cl@ve en el Punto de Acceso General http://administracion.gob.es.

V.2 Modalidad de identificación Cl@ve ocasional (Cl@ve PIN).

La AEAT actuará como organismo principal responsable del sistema de acceso basado en Cl@ve ocasional.

A tales efectos, la AEAT será la entidad encargada de realizar las funciones de identificación y autenticación de usuarios en esta modalidad de identificación, disponiendo de los medios necesarios para ello.

En consecuencia, la AEAT será responsable del funcionamiento del sistema de acceso basado en Cl@ve ocasional descrito en estas Prescripciones Técnicas así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito de la modalidad de identificación Cl@ve ocasional.

V.3 Modalidad de identificación Cl@ve permanente

La Gerencia de Informática de la Seguridad Social (GISS) actuará como organismo responsable del funcionamiento del sistema de acceso basado en Cl@ve permanente.

A tales efectos, la GISS será la entidad encargada de realizar las funciones de identificación y autenticación de usuarios en esta modalidad de identificación, disponiendo de los medios necesarios para ello, entre los que se cuenta una copia replicada del fichero de usuarios del sistema Cl@ve, necesario para verificar la identidad y las garantías de acceso.

En consecuencia, la GISS será responsable del funcionamiento del sistema de acceso basado en Cl@ve permanente descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito de la modalidad de identificación Cl@ve permanente.

V.4 Emisión de certificados electrónicos centralizados para firma mediante la plataforma Cl@ve.

La entidad encargada de realizar las funciones de emisión y custodia de certificados electrónicos centralizados de usuarios para firma mediante la plataforma Cl@ve será, en el ejercicio de sus competencias, la Dirección General de la Policía (DGP), de acuerdo a la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad y al Real decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica.

Para realizar estas funciones, la DGP utilizará la Infraestructura de Clave Pública correspondiente al DNI electrónico actualmente existente.

La DGP, en el ejercicio de sus competencias, es responsable del funcionamiento del servicio de emisión y custodia de certificados electrónicos centralizados de usuarios, actuando como prestador de servicios de confianza de acuerdo con el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, y conforme a los principios de seguridad, integridad, confidencialidad, autenticidad y no repudio previstos en la Ley 59/2003 de 19 de diciembre de Firma electrónica, y en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

V.5 Gestión de certificados electrónicos centralizados para firma mediante la plataforma Cl@ve.

La entidad encargada de realizar las funciones de almacenamiento y gestión de certificados electrónicos centralizados de usuarios para el sistema Cl@ve será la DGP.

Este organismo estará habilitado y dispondrá de los medios necesarios para realizar las funciones de almacenamiento y gestión de certificados descrita. Igualmente dispondrá de una copia replicada del fichero de certificados electrónicos indicado.

La GISS actuará como prestador de servicios de firma con certificado electrónico centralizado, para lo cual dispondrá de un respaldo de aquella información almacenada y

gestionada por la DGP necesaria para la firma. Dicha información estará sujeta a los siguientes requisitos:

a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;

b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio.

La DGP es responsable del funcionamiento del servicio de almacenamiento y gestión de certificados descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para este servicio.

V.6 Firma de documentos electrónicos mediante certificados electrónicos centralizados.

La entidad encargada de gestionar el entorno de creación de firma electrónica, en nombre del firmante, de documentos electrónicos mediante certificados electrónicos centralizados será la GISS que actuará como organismo responsable de este servicio, en unión con la DGP. A tales efectos, ambas entidades serán las habilitadas y dispondrán de los medios necesarios para realizar dichas funciones de firma de documentos electrónicos.

En consecuencia, ambos organismos serán los responsables del funcionamiento del servicio de firma de documentos electrónicos mediante certificados electrónicos centralizados descrito en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para este servicio.

V.7 Punto de acceso al sistema Cl@ve.

La entidad encargada de realizar las funciones correspondientes a la provisión del punto de acceso al sistema Cl@ve, de desarrollar los componentes comunes para facilitar la integración con este punto de acceso, y de desarrollar los componentes de firma comunes para el acceso al servicio de firma mediante certificados electrónicos centralizados será la DTIC.

La DTIC será responsable del funcionamiento del punto de acceso al sistema Cl@ve, de los componentes comunes para facilitar la integración con este punto de acceso y de los componentes de firma comunes para el acceso al servicio de firma mediante certificados electrónicos centralizados descritos en estas Prescripciones Técnicas, así como de los sistemas de información, aplicaciones, organización y procedimientos utilizados para el sistema Cl@ve en el ámbito del punto de acceso y los componentes comunes de integración.

V.8 Garantía de alta disponibilidad.

Los organismos responsables del funcionamiento de los diferentes subsistemas que conforman Cl@ve establecerán un sistema de alta disponibilidad del servicio ofrecido.

V.9 Garantía de fiabilidad del entorno de creación de firma electrónica.

Los organismos responsables del funcionamiento de los diferentes subsistemas que conforman Cl@ve aplicarán procedimientos de seguridad específicos en materia de gestión y administración, y utilizarán sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante.

VI. Adhesión al sistema Cl@ve

El ámbito de aplicación del sistema Cl@ve podrá extenderse a otras Administraciones Públicas, mediante la formalización de un convenio al efecto con el Ministerio de Hacienda y Administraciones Públicas. En dicho convenio se establecerán las condiciones técnicas, económicas y organizativas de aplicación a otras Administraciones Públicas que complementarán, en su caso, a las establecidas en las presentes Prescripciones Técnicas.

VII. Sistema de identificación e imputación de costes

Con objeto de garantizar la sostenibilidad del sistema Cl@ve, se implementarán mecanismos para identificar y eventualmente imputar los costes de mantenimiento y

explotación del sistema a las diferentes entidades usuarias, basados en el uso efectivo del mismo por parte de dichas entidades.

Para ello, desde la DTIC se llevará un censo de las entidades integradas con el Punto de Acceso del sistema Cl@ve, de modo que únicamente las entidades incluidas en el censo puedan hacer uso del mismo. Cada petición de identificación y autenticación recibida por el Punto de Acceso se asociará a una entidad usuaria a través del identificador de entidad emisora que deberá incluirse en dichas peticiones, dejando una traza en el registro de actividad del sistema. Dichas trazas, que contendrán para cada petición la entidad emisora, el resultado y la modalidad de identificación utilizada, serán objeto de tratamiento para determinar el uso efectivo del sistema realizado por cada entidad y por consiguiente para realizar la imputación de costes.

Asimismo, para las funciones de firma de documentos electrónicos mediante certificados electrónicos centralizados, las entidades participantes en la provisión del servicio, GISS y DGP, implementarán un sistema de identificación e imputación de costes equivalente al anterior, basado en un censo de entidades integradas con el sistema de firma y un registro de actividad en el que se almacenarán las trazas de las peticiones de firma mediante certificados electrónicos centralizados recibidas.

ANEXO I

Procedimientos de registro, acceso al sistema y firma electrónica de documentos

Se describen a continuación los procedimientos inicialmente previstos en relación al registro de usuarios, así como de acceso al sistema y firma de documentos electrónicos. Estos procedimientos podrán ser adaptados de acuerdo a las necesidades y a la evolución del sistema Cl@ve para una mejor prestación del servicio a los ciudadanos.

La información actualizada de los procedimientos podrá encontrarse en www.clave.gob.es.

1. Procedimientos de alta en el registro.

Existirán tres procedimientos de registro diferenciados en el sistema Cl@ve: registro telemático sin certificado electrónico reconocido, registro telemático con DNI electrónico o certificado electrónico reconocido, y registro presencial.

1.1 Registro telemático sin certificado electrónico reconocido.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Básico.

Este procedimiento de registro se inicia mediante la solicitud por parte del ciudadano ante la entidad responsable del Registro, o a instancias de esta última sin solicitud previa, utilizando para esta identificación inicial del ciudadano un dato conocido por el ciudadano y la entidad. Una vez verificada la identidad, se remitirá a la dirección postal del ciudadano que conste en la entidad responsable del registro una carta de invitación al sistema Cl@ve, en la que se incluirá un código seguro de verificación (CSV).

Una vez recibida la carta, el ciudadano puede acceder a la aplicación de registro en Cl@ve, donde se le solicitan los datos personales necesarios para completar el registro, así como el código CSV de la comunicación emitida. Como medida de seguridad adicional en el momento del registro, también se solicitará un dato de verificación conocido por el ciudadano y la entidad.

Como respuesta, se emite un acuse de recibo firmado electrónicamente por el sistema con un CSV que incluye los datos proporcionados, y que incluirá el código de activación asociado al registro realizado.

1.2 Registro telemático con DNI electrónico o certificado electrónico reconocido.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Avanzado

Los ciudadanos con certificado electrónico reconocido o DNIe, podrán formalizar el registro en el sistema Cl@ve mediante una aplicación web sin necesidad de acudir a ninguna oficina.

El ciudadano accederá al punto de registro telemático de Cl@ve y se identificará con su certificado reconocido o DNIe. La aplicación de registro tomará del certificado los datos identificativos del ciudadano, y los verificará contra los que figuren en su DNI. Puesto que se tomarán como ciertos para su incorporación al registro los datos correspondientes al DNI, si los datos del DNI y del certificado no coinciden exactamente, se informará de esta discrepancia al ciudadano para que efectúe las correcciones pertinentes en la información proporcionada.

A continuación se le pedirán los otros datos necesarios para el registro, incluidos su número de teléfono móvil y su dirección de correo electrónico y firmará con su certificado esta solicitud, incluyendo la selección de la casilla donde declara haber leído y estar de acuerdo con los términos y condiciones de uso.

Se le dará un acuse de recibo firmado por el sistema con los datos proporcionados, documento que incluirá el código de activación asociado al registro realizado. El sistema informará al usuario de la utilidad del código de activación y se recalcará la importancia de su conservación para poderlo usar como factor de autenticación en caso de olvido de contraseña.

1.3 Registro presencial.

Esta modalidad de registro se corresponde con un Nivel de garantía de registro Avanzado

El ciudadano podrá registrarse en persona en cualquiera de las oficinas de registro autorizadas del sistema Cl@ve. Estas oficinas contarán con una aplicación de registro que les permitirá, una vez identificado el ciudadano ante un empleado público, formalizar el registro. Para asegurar el estricto control por parte del usuario de los medios de identificación utilizados en el sistema, no se permitirá que el registro presencial sea realizado por una persona en representación de otra.

El proceso de registro presencial se realizará de acuerdo con lo establecido en la Resolución de la Dirección de Tecnologías de la Información y las Comunicaciones por la que se establecen las condiciones para actuar como oficina de registro presencial del sistema Cl@ve.

1.4 Bienvenida al sistema Cl@ve.

Una vez completado el registro en Cl@ve en cualquiera de las modalidades descritas anteriormente, el ciudadano recibirá, en el número de teléfono que acaba de registrar, un SMS de bienvenida al sistema.

A partir de la recepción de dicho SMS, el ciudadano registrado puede ya utilizar el sistema Cl@ve PIN y acceder a los sistemas de activación de contraseña del sistema Cl@ve permanente.

1.5 Obtención de nivel avanzado de garantía de registro.

Determinados servicios de Administración Electrónica requieren que el registro en Cl@ve se haya realizado con un nivel de garantía de registro avanzado, esto es, de forma presencial o telemáticamente con DNI electrónico o certificado electrónico reconocido.

Los ciudadanos que se hayan registrado en Cl@ve de forma telemática con una carta de invitación con un código seguro de verificación (CSV), y que por tanto dispongan únicamente de un nivel de garantía de registro básico, podrán solicitar la obtención del nivel avanzado personándose en las oficinas de registro o accediendo mediante DNIe o certificado electrónico reconocido a los sistemas de registro de Cl@ve.

1.6 Tratamiento del procedimiento de alta de un número de teléfono ya registrado.

El tratamiento descrito a continuación es común a los tres procedimientos de alta descritos anteriormente.

Por motivos de seguridad, el sistema requiere que un número de teléfono esté asignado a un único ciudadano usuario del sistema Cl@ve. En el caso de que un ciudadano intente registrarse con un teléfono que ya está dado de alta en el sistema asignado a otro usuario registrado, se seguirá este procedimiento para completar el registro:

1. Se explicará al ciudadano la situación detectada y se enviará un SMS con un código de un solo uso al número de teléfono móvil que se pretende registrar para que el usuario, o en su caso el empleado público que atiende el registro presencial, lo aporte en ese mismo momento para demostrar que el ciudadano es el poseedor del teléfono.

2. El sistema comprobará la validez del código de un solo uso aportado y en el caso de ser correcto se completará el registro y se procederá a revocar el número de teléfono al usuario que lo tenía anteriormente asignado. En caso contrario no se podrá completar el proceso de registro.

3. El usuario cuyo número de teléfono haya sido revocado en aplicación de este procedimiento no causará baja en el sistema Cl@ve, pero no podrá hacer un uso efectivo del mismo. Si el usuario intenta acceder al sistema se le informará que su usuario ha sido revocado por razones de seguridad con el fin de garantizar una asociación única con el número de teléfono móvil, y se le invitará a subsanar esta incidencia aportando un nuevo número de teléfono mediante el procedimiento establecido al efecto.

4. A los exclusivos efectos de informar al usuario que ha sido revocado su número de teléfono en aplicación de este procedimiento, el sistema podrá utilizar alguno de los datos de contacto incluidos en la Base de Datos de Registro para comunicarle esta incidencia y que pueda proceder a subsanarla, en su caso.

2. Procedimientos de baja en el registro.

Se habilitarán tres procedimientos de baja en el sistema Cl@ve:

2.1 Procedimiento de baja por renuncia.

El ciudadano puede renunciar a la utilización del sistema Cl@ve en cualquier momento, incluso aunque no se haya dado de alta en el mismo.

La renuncia podrá llevarse a cabo en el portal www.clave.gob.es, identificándose ante él y eligiendo en las opciones de usuario la de renuncia al sistema. En este caso el sistema deberá mostrar primero una pantalla de aviso para informar al usuario de que ya no podrá acceder al sistema y que si posteriormente quiere darse da alta deberá proceder de nuevo al procedimiento de registro como usuario. Si el ciudadano confirma esta pantalla, el sistema marcará al usuario como dado de baja por renuncia. Indistintamente podrá realizar esta petición usando DNIe o certificado electrónico reconocido o de manera presencial en una oficina. Si el registro se ha realizado a nivel básico, mediante carta de invitación, la renuncia también se podrá tramitar mediante el código CSV incluido en la misma.

Si un ciudadano renuncia al sistema, se revocará su certificado electrónico centralizado, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica Cl@ve.

2.2 Procedimiento de revocación de oficio.

El sistema Cl@ve podrá gestionar la revocación de oficio de usuarios registrados en el sistema cuando concurran circunstancias que pongan en riesgo la seguridad del mismo, como un uso fraudulento o desleal del sistema o cuando se produzca una modificación sustancial de los datos de identificación utilizados en el registro, como son el cambio del nombre o los apellidos en su DNI o la nacionalización o expulsión de extranjeros.

A los exclusivos efectos de informar al usuario que ha sido revocado en aplicación de este procedimiento, el sistema podrá utilizar alguno de los datos de contacto incluidos en la Base de Datos de Registro para comunicarle esta incidencia.

La revocación solo podrá dar lugar a una nueva alta cuando se hayan modificado las circunstancias que motivaron la misma.

Los efectos de la revocación serán los mismos que los de la renuncia, de forma que se revocará su certificado electrónico centralizado, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica de Cl@ve.

2.3 Procedimiento de baja por fallecimiento.

El sistema Cl@ve gestionará automáticamente y de oficio la baja de los usuarios fallecidos de los que se tenga constancia y se encuentren registrados. Los efectos de la baja

por fallecimiento serán los mismos que los de la renuncia: se revocará el certificado electrónico centralizado del usuario, caso de existir, y se deshabilitará su acceso electrónico tanto mediante Cl@ve PIN como mediante Cl@ve Permanente a los servicios de identificación, autenticación y firma electrónica de Cl@ve.

3. Procedimientos de modificación de datos en el registro.

Se habilitarán los siguientes procedimientos de modificación de datos del registro:

3.1 Procedimiento de modificación del número de móvil.

Si el ciudadano desea modificar el número de móvil que notificó durante el acto del registro, deberá acudir de nuevo a una oficina de registro donde le actualizarán, previa identificación con su DNI, TIE o Certificado de Ciudadano de la Unión Europea, el número de teléfono móvil en la base de datos y le proporcionarán un nuevo código de registro para futuras operaciones, teniendo que firmar de nuevo el correspondiente documento de aceptación. También podrá hacer la operación de forma telemática, si el usuario dispone de un certificado electrónico reconocido o DNIe.

En el caso de que el nuevo número de teléfono móvil ya esté dado de alta en el sistema, se aplicará el procedimiento de alta de un número de móvil ya registrado descrito anteriormente.

El procedimiento de modificación del número de móvil no implica la revocación del certificado electrónico centralizado del ciudadano ni la desactivación de su usuario y contraseña de acceso.

3.2 Procedimiento de modificación de otros datos.

El usuario registrado en el sistema puede modificar otros datos asociados al registro, a excepción del número de DNI y del nombre y los apellidos.

Estas modificaciones se podrán realizar telemáticamente en el portal www.clave.gob.es o en una de las oficinas de registro.

El procedimiento de modificación de estos datos no generará un nuevo código de activación aunque sí el documento de aceptación de condiciones, donde se incluirán los nuevos datos declarados por el ciudadano.

4. Procedimiento de uso de Cl@ve PIN.

En la Modalidad de Identificación Cl@ve ocasional, el usuario aportará la primera parte de su clave y recibirá un código en su dispositivo móvil, de validez muy limitada en el tiempo, que conjuntamente conforman el código de acceso.

Para reforzar la seguridad del sistema de identificación y autenticación se divide el código de acceso (Cl@ve PIN) en dos partes:

• Clave de acceso: la define el usuario cada vez que solicita un Cl@ve PIN. No tiene que ser siempre la misma.
• PIN: la envía el sistema Cl@ve al móvil del usuario cuando lo solicita.

De manera que la unión de ambos datos conforma el Código de Acceso.

Código de Acceso (Cl@ve PIN) = Clave de Acceso + PIN.

Este sistema permite al ciudadano tener el control sobre una parte del código de acceso de forma que es el usuario quien lo define cada vez que solicita un PIN. Como medida de seguridad adicional, este código nunca se envía en claro al sistema Cl@ve. De esta manera, se logra que, aunque otra persona pudiera tener acceso a estos mensajes, no podría suplantar al usuario pues le faltaría conocer la parte del código que define el propio usuario.

Se definen los siguientes procedimientos relativos a la obtención y utilización del sistema Cl@ve PIN:

4.1 Procedimiento de obtención de Cl@ve PIN.

Para la obtención de un PIN en el sistema Cl@ve, el solicitante deberá acceder al portal de gestión de la Cl@ve ocasional, donde deberá introducir su usuario Cl@ve (número del DNI o NIE), información de contraste conocida por ambas partes, elegir una clave de acceso, que no es necesario que sea siempre la misma, y solicitar un nuevo PIN. Como resultado, el

sistema Cl@ve enviará un código al teléfono móvil registrado con el que el usuario podrá completar la autenticación.

4.2 Procedimiento de utilización de Cl@ve PIN.

Para completar la autenticación en el sistema el usuario deberá introducir su usuario Cl@ve (DNI o NIE) y su código de acceso formado por la clave seleccionada en el momento de la obtención y el PIN recibido en su teléfono móvil.

Si el solicitante introduce erróneamente el código de acceso más veces de las permitidas, por motivos de seguridad, se bloqueará el acceso de forma temporal.

La validez del PIN es la siguiente:

• Validez temporal: Se deberá utilizar el PIN que se ha recibido en el teléfono móvil para completar el acceso al sistema antes de 10 minutos. Pasado ese tiempo, si no se ha llegado a acceder a Cl@ve, se deberá solicitar un nuevo PIN.

• Número de usos: El PIN se configura como una clave de un solo uso (OTP), de forma que se garantice que siempre que se solicite una autenticación con Cl@ve PIN se fuerce al usuario a iniciar el proceso de solicitud de un nuevo PIN para poder autenticarse en esa sesión.

• Sesión: Una vez identificado mediante Cl@ve PIN se puede acceder a los servicios que permitan Cl@ve hasta que se produzca la desconexión de la Sede Electrónica o se cierre el navegador.

5. Procedimientos de activación y gestión de contraseñas.

Se definen los siguientes procedimientos relativos a la activación de cuentas de usuario en el sistema Cl@ve y gestión de las contraseñas:

5.1 Procedimiento de activación.

Para la activación de la cuenta de usuario en el sistema Cl@ve, necesaria para poder utilizar la modalidad de identificación de Cl@ve permanente, el solicitante deberá acceder al portal www.clave.gob.es, donde deberá introducir su identificador de usuario Cl@ve (DNI o NIE), su dirección de correo electrónico y el código de activación que se le ha suministrado en el acto del registro. Si son correctos, el sistema le enviará un mensaje al móvil con un código de un solo uso que el usuario deberá introducir en el sistema y, una vez comprobado, le permitirá introducir la contraseña que prefiera para acceder ulteriormente a Cl@ve, cumpliendo con las características mínimas de seguridad definidas.

Si el solicitante introduce erróneamente el código de activación más veces de las permitidas, el código de activación quedará bloqueado por motivos de seguridad y se precisará la generación de uno nuevo.

5.2 Procedimiento de cambio de contraseña.

Las contraseñas de los usuarios caducarán en el plazo determinado por la política de seguridad del sistema, plazo que se comunicará en el portal www.clave.gob.es. En cualquier caso, el usuario podrá cambiar la contraseña de acceso en cualquier momento. Para ello accederá al sistema con su usuario y contraseña y dentro de las opciones de usuario elegirá cambiar contraseña. Introducirá la nueva contraseña y el sistema le enviará un código de un solo uso al móvil para confirmar la operación.

Esta operación podrá realizarse también accediendo con DNIe o certificado reconocido, en cuyo caso no hará falta el código de un solo uso.

5.3 Procedimiento de restablecimiento de contraseña.

Este procedimiento será necesario si el ciudadano olvida su contraseña o ésta queda bloqueada al producirse el número máximo de intentos fallidos en la introducción de la misma. En tal caso habrá de establecerse una contraseña nueva.

Para restablecer la contraseña, el ciudadano accederá al sistema con su usuario y seleccionará la opción de «restablecimiento de contraseña». El sistema le pedirá el código de activación que se le entregó en el proceso de registro y que deberá coincidir con el que consta en la base de datos. Si es correcto, el sistema enviará un código de seguridad al móvil del ciudadano, código que deberá introducir para restablecer la contraseña.

5.4 Procedimiento de recuperación del código de activación.

Si el usuario desea restablecer la contraseña y no dispone del código de activación, podrá obtener un nuevo código de activación acudiendo a una oficina de registro o telemáticamente autenticándose mediante certificado electrónico reconocido o DNIe o mediante Cl@ve PIN. Esta operación no precisa la emisión del documento de aceptación puesto que el ciudadano no está declarando ningún dato nuevo.

6. Procedimientos de gestión de certificados y firma electrónica.

Los siguientes procedimientos son de aplicación en relación a los certificados electrónicos centralizados para firma.

6.1 Procedimiento de emisión de los certificados centralizados para firma con la plataforma Cl@ve.

Una vez que el usuario se ha registrado en el sistema con nivel avanzado de garantía de registro, ha activado su Cl@ve Permanente, y ha solicitado expresamente la emisión de sus certificados electrónicos centralizados para firma mediante la plataforma Cl@ve, dicha emisión se llevará a cabo la primera vez que el ciudadano acceda al procedimiento de firma con el sistema Cl@ve.

El sistema informará al ciudadano de que se le va a emitir su certificado, así como de las garantías de seguridad ofrecidas por la Administración para la custodia y acceso al mismo, y generará en ese momento su clave privada y la almacenará en el sistema de forma protegida, de modo que se garantice, con un alto nivel de confianza, su uso bajo el control exclusivo de su titular.

La generación de los certificados deberá hacerse acorde con los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial.

6.2 Procedimiento de firma con certificado electrónico centralizado.

El procedimiento de firma electrónica con certificado electrónico centralizado garantizará que el acceso a los datos de creación de firma asociados al certificado sólo sea efectuado por el titular del mismo, por lo que para su uso se deberá haber autenticado previamente al ciudadano mediante dos factores de autenticación: la pareja identificador de Cl@ve con su contraseña de Cl@ve permanente, y un código de un solo uso (OTP) enviado por SMS a su móvil.

6.3 Procedimiento de renovación de los certificados electrónicos centralizados.

La renovación de los certificados centralizados para firma mediante la plataforma Cl@ve se podrá llevar a cabo de forma automática siempre y cuando se cumplan los requisitos que la ley marca con respecto a los plazos máximos permitidos desde que el ciudadano realizó el registro presencial. En caso contrario, para renovar su certificado el ciudadano tendrá que personarse en una oficina de registro para que se le provea de un nuevo código de activación y pueda volver a activarse su usuario y sus certificados.

La renovación automática se producirá cuando el ciudadano se disponga a firmar, se haya autenticado para poder acceder a su clave de firma y se detecte en ese momento que su certificado está caducado o próximo a caducar, hasta 2 meses antes de la fecha de expiración de su validez. En ese caso el sistema Cl@ve emitirá y almacenará automáticamente los nuevos certificados revocando previamente los antiguos, de acuerdo a la normativa vigente sobre certificados electrónicos reconocidos.

En todo caso el sistema informará al ciudadano de que se ha procedido a la renovación automática de sus certificados y le comunicará el nuevo periodo de validez de los mismos, informando también de que los anteriores certificados han sido revocados, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto.

6.4 Procedimiento de revocación.

La revocación de los certificados electrónicos centralizados del ciudadano se llevará a efecto en caso de renuncia o baja voluntaria del ciudadano en el sistema, en el caso de baja

por fallecimiento y en el caso de revocación de oficio del acceso al sistema llevada a cabo por la Administración en las circunstancias que se determinen.

Una vez revocado un certificado, el sistema garantizará que no se podrá utilizar a partir de ese momento durante un proceso de firma.

El sistema podrá permitir también, con las garantías que se consideren necesarias, que el propio ciudadano pueda solicitar tanto presencial como telemáticamente la revocación exclusiva de su certificado electrónico de firma centralizado, sin necesidad de darse de baja en el sistema Cl@ve. La revocación deberá constatarse documentalmente, por lo que en cualquiera de estos procedimientos el ciudadano deberá firmar la solicitud de renuncia o revocación, ya sea con un certificado electrónico reconocido o de forma manuscrita.

7. Procedimientos de incorporación de registros de otros censos.

Tal y como establece el Acuerdo del Consejo de Ministros de creación de Cl@ve, para incorporar al Censo Cl@ve usuarios registrados en otros sistemas de identificación, autenticación y firma que existan con anterioridad al propio acuerdo, se deberá solicitar el consentimiento expreso del ciudadano.

En cualquier caso, los procedimientos de incorporación asegurarán que en estos censos se han cumplido los requisitos necesarios para poder asignar el nivel de garantía de registro y el sistema de identificación y autenticación correspondientes en el sistema Cl@ve. Asimismo, el procedimiento deberá permitir comprobar la veracidad y exactitud de los datos aportados desde los otros censos y se solicitará al usuario la aportación de los datos complementarios necesarios para completar el registro, todo ello manteniendo las mismas garantías que aplican al procedimiento de alta de usuarios en el sistema Cl@ve.

Se integrarán en una primera fase los censos del sistema PIN24H de la AEAT y del sistema usuario-contraseña de la Seguridad Social. En cualquier caso, la incorporación de registros de otros censos requerirá la autorización de la DTIC.

§ 18

Resolución de 23 de febrero de 2022, de la Secretaría General de Administración Digital, por la que se establecen las condiciones de uso de firma electrónica no criptográfica vinculada a "AutenticA", para la relación con la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 56, de 7 de marzo de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-3527

AutenticA es un servicio, desarrollado y gestionado por la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital, para la autenticación y autorización de usuarios en el acceso a determinados procedimientos de administración electrónica en el ámbito de la Administración General del Estado y sus organismos públicos o entidades de derecho público vinculados o dependientes. Se trata de un servicio de identidad digital basado en un repositorio horizontal de usuarios procedentes de fuentes primarias con las que se sincroniza y, en la actualidad, ofrece una capa horizontal de autenticación con certificado electrónico, y otros medios de autenticación como usuario y contraseña, lo cual favorece la interoperabilidad y la seguridad del sistema.

Hasta el momento, en los procedimientos electrónicos y trámites en los que en la fase de identificación los interesados o usuarios son autenticados a través de AutenticA, en el momento de completar la actuación concreta que requiera firma electrónica de dicho interesado o usuario sólo pueden firmar electrónicamente por medio de firma electrónica avanzada basada en certificados cualificados.

El Reglamento (UE) N.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica (en adelante Reglamento eIDAS) y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, establecen las condiciones de uso de la firma electrónica avanzada basada en certificados cualificados. Esta firma se encuentra muy extendida en el ámbito de la administración digital (por ejemplo es el sistema de firma de la suite «@firma», entre otras aplicaciones) y se basa en tecnología y herramientas muy consolidadas. Sin embargo, la práctica ha demostrado que elevada variedad de equipos, de escritorio o en movilidad, versiones de sistemas operativos, navegadores y, en su caso, máquinas virtuales Java, provoca que, en determinadas circunstancias, la firma del interesado o usuario

mediante certificados cualificados sea muy gravosa o, en el peor de los casos, no sea técnicamente viable.

Para dar respuesta a esta situación no deseada en caso de que se produzca y poder extender así el uso de los servicios electrónicos, se considera conveniente disponer, de forma complementaria a la firma electrónica avanzada, de un sistema de firma electrónica básica vinculada a AutenticA que no requiera el procedimiento de firma electrónica local y que, gracias a ello, pueda ser operativa en un contexto como el mencionado, sistema que resultará apropiado aun cuando se haya utilizado un certificado electrónico en el proceso de identificación.

A estos sistemas de firma electrónica han de reconocérsele efectos jurídicos y son conformes a lo establecido en el artículo 25.1 del Reglamento eIDAS, sin perjuicio de lo previsto en el artículo 27 de la propia norma, que regula las «Firmas electrónicas en servicios públicos».

Con relación a los potenciales usuarios de la firma electrónica no criptográfica a que se refiere esta Resolución, debe tenerse en cuenta un triple marco normativo:

En primer lugar, el artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece que cada Administración Pública determinará los sistemas de firma electrónica que debe utilizar su personal. Así, la firma electrónica no criptográfica a que se refiere esta Resolución permitirá una mayor cobertura de los servicios de administración digital orientados a los empleados públicos de la Administración General del Estado, como es el caso de los provistos por la Sede Funciona, creada según Orden TFP/303/2019, de 12 de marzo, y su versión móvil, o bien en el Portal Funciona, a través de Red SARA, ofrecidos por el Sistema Integrado de Gestión de Personal y el Registro Central de Personal.

En segundo lugar, la disposición adicional primera del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por Real Decreto 203/2021, de 30 de marzo, establece la obligatoriedad de uso de medios electrónicos en los procesos selectivos para el acceso al empleo público en el ámbito de la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes de la misma. La elección de puestos de primer destino, ofrecido por el Sistema Integrado de Gestión de Personal, para los aspirantes que hayan aprobado un proceso selectivo en este ámbito requiere su firma electrónica, que se llevará a cabo mediante los sistemas previstos en el artículo 10.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, bien mediante un certificado electrónico cualificado de firma electrónica a que se refiere el párrafo a) o bien un sistema de firma objeto de esta Resolución en aplicación de lo previsto en el párrafo c).

En tercer lugar, los sujetos obligados por la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo en la Administración General del Estado, se relacionan con la Oficina de Conflictos de Intereses exclusivamente por medios electrónicos para la presentación de todas las declaraciones y el resto de comunicaciones y documentos a través de la sede electrónica asociada del Portal FUNCIONA, de acuerdo con lo previsto en el artículo 3 y en la disposición final primera del Reglamento por el que se desarrollan los títulos Preliminar, II y III de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, aprobado por el Real Decreto 1208/2018, de 28 de septiembre.

El Esquema Nacional de Seguridad (en adelante ENS) regulado por el Real Decreto 3/2010, de 8 de enero, constituye el marco legal que permite definir y establecer las medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita a los firmantes y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En la implantación de un sistema de firma electrónica no criptográfica se deberá cumplir con el ENS para garantizar la seguridad de los datos y los servicios, como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.

El ENS establece la necesidad de categorizar los sistemas de información, siendo la categoría de un sistema de información, en materia de seguridad, la que permite modular el equilibrio entre la importancia de la información que maneja, los servicios que presta y el

esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

En virtud de lo anterior, y de acuerdo con el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital, esta Secretaría General de Administración Digital, en el ejercicio de las competencias atribuidas para definición de estándares, de directrices técnicas y de gobierno TIC (Tecnologías de la Información y las Comunicaciones), de normas de calidad e interoperabilidad de aplicación a las Administraciones Públicas y el desarrollo y aplicación de lo dispuesto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica y sus Normas Técnicas de Interoperabilidad, y con el informe favorable preceptivo y vinculante de la Secretaría de Estado de Seguridad del Ministerio del Interior previsto en el art. 10.2.c) de la Ley 39/2015, de 1 octubre, evacuado el 25 de enero de 2022, dispone:

Primero.

1. Aprobar los términos y condiciones de uso de la firma electrónica no criptográfica vinculada a AutenticA, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el artículo 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los títulos Preliminar, II y III de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, y sus respectivos desarrollos reglamentarios, así como en la Disposición adicional segunda de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

2. Ordenar su publicación en el «Boletín Oficial del Estado».

Segundo.

La presente Resolución entra en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Términos y condiciones de uso de la firma electrónica no criptográfica vinculada a AutenticA

Primero. *Objeto.*

Los presentes términos y condiciones tienen como objeto determinar los supuestos en que un sistema de firma electrónica no basada en certificados electrónicos vinculada al servicio AutenticA podrá ser utilizado en el ámbito de la Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes de la misma, de acuerdo con lo previsto en el artículo 43.2 de la Ley 40/2015, de 1 de octubre, el artículo 10 de la Ley 39/2015, de 1 de octubre, y los títulos Preliminar, II y III de la Ley 3/2015, de 30 de marzo. Todo ello sin perjuicio, de otros sistemas de firma implantados, que ofrezcan las garantías de seguridad suficientes para gestionar la integridad y el no repudio, según el principio de proporcionalidad recogido en el artículo 13.3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, que regula el análisis y gestión de los riesgos en dicho ENS.

Segundo. *Ámbito de aplicación.*

La firma electrónica no criptográfica vinculada a AutenticA prevista en esta Resolución se podrá utilizar en actuaciones o procedimientos de administración electrónica que permitan el uso de la firma electrónica básica, entre otros:

a) Los servicios de administración digital provistos por la Sede Funciona, creada según Orden TFP/303/2019, de 12 de marzo, y su versión móvil, o bien en el Portal Funciona, a través de Red SARA, que están orientados a los empleados públicos de la AGE, ofrecidos por el Sistema Integrado de Gestión de Personal y el Registro Central de Personal.

b) El servicio de elección de puestos de primer destino, ofrecido por el Sistema Integrado de Gestión de Personal, para los aspirantes que hayan aprobado un proceso selectivo.

c) Los servicios de declaraciones y comunicaciones del personal alto cargo, disponibles en la Sede Funciona, y dirigidas a la Oficina de Conflictos de Intereses, conforme al Real Decreto 1208/2018, de 28 de septiembre, por el que se aprueba el Reglamento por el que se desarrollan los títulos preliminar, II y III de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

d) En cualquier servicio disponible en la Sede Funciona que permita la relación con la Administración General del Estado, por parte de empleados públicos en situación de excedencia o servicios especiales.

e) En el servicio TRAMA, de gestión de permisos e incidencias y control de presencia de personal, gestionado por la Secretaría General de Administración Digital.

Tercero. *Criterios para la utilización de la firma no criptográfica vinculada a AutenticA.*

En aplicación del Real Decreto 3/2010, de 8 de enero, se podrá utilizar un sistema de firma electrónica no criptográfica vinculada a AutenticA cuando el sistema de información asociado al procedimiento o servicio electrónico haya sido categorizado, según el ENS, de categoría BÁSICA y aquellos de categoría MEDIA en los que no sea necesario utilizar la firma avanzada, cuando así lo disponga la normativa reguladora aplicable.

Cuarto. *Garantía de funcionamiento.*

1. Cuando la actuación realizada por el usuario del servicio AutenticA, en su relación con la Administración General del Estado y sus organismos públicos y entidades de Derecho Público vinculados o dependientes de la misma, implique la presentación en una sede electrónica o sede electrónica asociada de documentos electrónicos utilizando un sistema de firma electrónica contemplado en la presente Resolución, se garantizará la integridad de la información presentada mediante el sellado realizado con un sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, a la que se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y su incorporación inmediata al sistema de información asociado al procedimiento o servicio electrónico.

La Administración General del Estado, sus organismos públicos o entidades de derecho público vinculados o dependientes de la misma deberán disponer de las medidas técnicas, organizativas y procedimentales necesarias para garantizar dicha integridad a lo largo del tiempo de igual manera que se hace en los casos de firma criptográfica.

2. Asimismo, se garantizará también la integridad de las evidencias necesarias para la verificación de la identidad, recopiladas inmediatamente antes del acto de la firma, así como, posteriormente, del consentimiento explícito del firmante con el contenido firmado, almacenando dichas evidencias junto con la información presentada. La integridad y conservación de los documentos electrónicos almacenados y de sus metadatos asociados obligatorios quedará garantizada a través del sellado con el sello electrónico cualificado del organismo y del resto de medidas técnicas que aseguren su inalterabilidad, de acuerdo con lo previsto en el apartado anterior.

3. En los supuestos previstos en los párrafos a) a d) del apartado segundo de esta Resolución, los sistemas a los que se refiere esta resolución facilitarán a la persona firmante un justificante de firma sellado con un sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, y acompañado de un el código seguro de verificación, o CSV, que será el documento con valor probatorio de la actuación realizada.

La integridad de los documentos electrónicos autenticados mediante CSV podrá comprobarse mediante el acceso directo y gratuito a la sede electrónica del Punto de Acceso General de la Administración General del Estado o en la Sede Funciona, en tanto no se destruyan de acuerdo con la normativa vigente.

Quinto. *Acreditación de la autenticidad de la expresión de la voluntad y consentimiento de la persona usuaria.*

1. Para acreditar la autenticidad de la expresión de la voluntad y consentimiento del firmante, se requerirá:

a) La autenticación del firmante, inmediatamente previa a la firma, utilizando el servicio AutenticA.

La autenticación, inmediatamente previa al acto de firma, deberá de hacerse con certificado electrónico u otro mecanismo que disponga de un nivel de calidad en la autenticación sustancial o alto, conforme a lo establecido en el Reglamento eIDAS.

b) La verificación previa por parte del firmante de los datos a firmar. Estos datos se obtendrán a partir de aquella información presentada por el firmante y de cuya veracidad se hace responsable, así como de los documentos electrónicos que, eventualmente, presente en el procedimiento o servicio electrónico que requiere la firma.

El firmante debe ser consciente de los datos que va a firmar y deberá ofrecérsele de un modo visible la posibilidad de consultarlo en un formato legible y, preferiblemente, con el mismo formato del documento que posteriormente se entregue al firmante como justificante de la firma.

c) La acción explícita por parte del firmante de manifestación de consentimiento y expresión de su voluntad de firma.

Cuando las aplicaciones hagan uso de los sistemas de firma previstos en esta Resolución, se deberá requerir de forma expresa la expresión del consentimiento y la voluntad de firma del firmante, mediante la inclusión de frases que pongan aquéllos de manifiesto de manera inequívoca, y la exigencia de acciones explícitas de aceptación por parte del firmante (por ejemplo, mediante una casilla junto al texto «Declaro que son ciertos los datos a firmar/muestro mi conformidad con el contenido del documento y confirmo mi voluntad de firmar» que el firmante debe marcar, y un botón «Firmar y enviar» que debe pulsar para realizar la firma).

Sexto. *Garantía de no repudio en el proceso de firma y gestión de las evidencias de autenticación.*

1. Para garantizar el no repudio de la firma por parte del firmante, un sistema de firma previsto en esta Resolución deberá acreditar la vinculación de la expresión de la voluntad y los datos firmados con la misma persona. Para ello, se volverá a solicitar la autenticación del firmante, mediante el servicio AutenticA, en el momento de proceder a la firma.

Asimismo, la garantía de no repudio exige que el sistema de firma asegure una adecuada trazabilidad en el caso de que sea necesario auditar una operación de firma concreta, para lo cual conservará, por cada firma y, por tanto, por cada proceso de autenticación, la siguiente información:

a) Fecha y hora de la autenticación.
b) Nombre y apellidos del firmante.
c) DNI/NIF/NIE del firmante.
d) Sistema de identificación sustancial o alto empleado.
e) Resultado exitoso de la autenticación.
f) Petición al proveedor externo de servicios de identificación o, en su caso, de validación y respuesta devuelta y firmada por éste.
g) Fecha y hora de la firma.
h) Resumen criptográfico de los datos firmados, realizado con un algoritmo de *hash* que cumpla las especificaciones del esquema nacional de seguridad.
i) Referencia al justificante de firma, en su caso, mediante el CSV asociado a dicho justificante.

La información a que se refieren los párrafos anteriores será sellada con un certificado de sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos. Adicionalmente, se añadirá un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo

supervisado, y será almacenada, como evidencia de la verificación de la identidad previa al acto de la firma, vinculada a los datos firmados.

En el caso de que los datos de identificación obtenidos en la autenticación inmediatamente anterior a la firma no coincidan con los datos de identificación obtenidos en autenticaciones previas, el sistema de firma no permitirá la realización de la misma, informando de esa eventualidad al sistema de información asociado al procedimiento o servicio electrónico que requiere dicha firma.

2. Con relación a la gestión de las evidencias de autenticación, a pesar de que el sistema de firma proporcionará a los sistemas de información asociados al procedimiento o servicio electrónico que requiere la firma la información relativa a la autenticación vinculada a dicha firma, en ocasiones puede ser necesario, por motivos de auditoría, recuperar las evidencias completas del proceso de autenticación.

En el caso de utilizar un sistema de identificación que requiera la consulta a un proveedor de servicios de identificación externo o a un proveedor de servicios de validación externo, las evidencias últimas no residen en el propio sistema de firma, sino en los sistemas de los proveedores de servicios de identificación o validación externos.

Con objeto de que los proveedores de esos servicios de identificación o validación puedan recuperar las evidencias necesarias para acreditar la realización de la identificación y autenticación previas ligadas a la realización de una firma en el sistema, se deberá facilitar a dichos proveedores la información de autenticación almacenada como evidencia de la verificación previa de la identidad en los sistemas de información asociados al procedimiento o servicio electrónico que requiere la firma, descrita en el apartado anterior.

A tal efecto, los proveedores de servicios de identificación o validación deberán salvaguardar dichas evidencias durante el plazo mínimo de cinco años. La solicitud de certificación de dichas evidencias se realizará conforme a la declaración de prácticas validación o declaración de política de certificación del proveedor.

Séptimo. *Garantía de la integridad de los datos y documentos firmados.*

1. Una vez acreditada la expresión de la voluntad y el consentimiento para firmar del firmante, se deberán establecer los mecanismos para garantizar la integridad e inalterabilidad de los datos y, en su caso, de los documentos electrónicos presentados por el firmante, para lo cual el sistema de firma sellará los datos a firmar, con un sello electrónico, conforme al artículo 19 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos y la adición de un sello de tiempo realizado con un certificado cualificado y emitido por un prestador de sellado de tiempo supervisado, y la pondrá a disposición del sistema de información asociado al procedimiento o servicio electrónico que requiere la firma.

2. En el proceso de firma se entregará al firmante bien el documento firmado electrónicamente, o bien, un justificante de firma, que será un documento legible, de acuerdo con la norma técnica de interoperabilidad de catálogo de estándares y preferiblemente en formato PDF y que deberá cumplir estos requisitos:

1.º Contener los datos del firmante tales como nombre, primer apellido y, en su caso, segundo apellido.

2.º Opcionalmente, contener los datos a firmar expresamente por el firmante, pudiendo contener una referencia de los documentos anexos, o, en su defecto, un hash del documento firmado.

3.º Garantizar la autenticidad del documento firmado, incluyendo en el justificante de firma un código seguro de verificación (CSV), y garantizando que este documento, o bien, el justificante, se pueda consultar en línea mediante un sistema de cotejo de CSV cuya dirección se incluya en el propio justificante de firma.

4.º En caso de que la consulta en línea, mediante código CSV, permita acceder al justificante de firma y no al documento firmado en sí, el justificante deberá contener los datos firmados expresamente por el firmante.

§ 19

Resolución de 6 de julio de 2023, de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por la que se publica el Acuerdo del Consejo de Ministros de 27 de junio de 2023, por el que se determinan los supuestos de validez de sistemas de identificación y firma electrónica en la Administración del Estado cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 166, de 13 de julio de 2023
Última modificación: sin modificaciones
Referencia: BOE-A-2023-16284

El Consejo de Ministros en su reunión del día 27 de junio de 2023, ha adoptado un Acuerdo por el que se determinan los supuestos de validez de sistemas de identificación y firma electrónica en la administración del Estado cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido.

A los efectos de dar publicidad al mencionado Acuerdo del Consejo de Ministros de 27 de junio de 2023, y de cumplir con el apartado tercero. Entrada en Vigor, esta Secretaría de Estado de Digitalización e Inteligencia Artificial ha resuelto disponer la publicación del mismo en el «Boletín Oficial del Estado» como anexo a la presente Resolución.

ANEXO

La Comunicación de la Comisión europea de 9 de marzo de 2021 titulada «Brújula digital 2030: el camino europeo para la década digital» prevé que para el año 2030 el 80% de los ciudadanos se beneficien del despliegue de una identidad digital fiable y controlada por el usuario, que le permitirá acceder a los servicios digitales en línea de los sectores público y privado, reforzando la privacidad y cumpliendo plenamente la legislación vigente en materia de protección de datos.

En este contexto, la Comisión europea adoptó la Recomendación (UE) 2021/946, de 3 de junio de 2021, sobre un conjunto de instrumentos común de la Unión para adoptar un enfoque coordinado de cara a un Marco para una Identidad Digital Europea. A partir de esta Recomendación, España viene participando en numerosos grupos de trabajo en aras de definir los requerimientos funcionales, técnicos y de seguridad en relación con una cartera digital que almacene credenciales verificables de identidad de los ciudadanos.

El Gobierno, en el marco del programa Europa Digital de la Unión Europea, lidera a través de la Secretaría General de Administración Digital (SGAD) del Ministerio de Asuntos Económicos y Transformación Digital los consorcios denominados Digital Credentials For

Europe (DC4EU) y EBSI Nodes Expansion (EBSI-NE) junto a más de un centenar de socios de 23 Estados Miembros europeos, además de Noruega y Ucrania. Ambos consorcios guardan una estrecha interrelación al construirse sobre la base de la tecnología Blockchain, elemento imprescindible en la nueva cartera digital europea que será objeto del piloto y que prevé tener un papel fundamental el desarrollo de los nuevos servicios digitales. En los trabajos que se están desarrollando en el marco del Toolbox eIDAS para la construcción de una Cartera Digital europea, el 9 de febrero de 2023 se aprobó el documento final de Architecture Reference Framework (ARF), según el cual el *wallet* ha de ser compatible con la especificación W3C Verifiable Credentials Data Model 1.1., que es la misma que se utiliza en el proyecto EBSI a la hora de emitir y validar credenciales verificables

Asimismo, el Plan de Digitalización de las Administraciones Públicas 2021-2025, que es uno de los elementos principales del Componente 11 (denominado «Modernización de las Administraciones Públicas») del Plan de Recuperación, Transformación y Resiliencia, incluye dentro de su Eje estratégico 1 («Transformación Digital de la Administración General del Estado») la Medida 4, que establece un nuevo modelo de identidad digital. Este nuevo modelo tiene por objeto desarrollar sistemas y servicios de identificación sencillos, seguros y usables por los ciudadanos, entre los que se encuentra el desarrollo de la «Cartera digital» española, que se incardina también en la revisión en curso del Reglamento eIDAS (el eIDAS 2). Respecto de la vinculación con el Plan de Recuperación, Transformación y Resiliencia, esta medida se incardina en el Componente 11, inversión I1 («Modernización de la Administración General del Estado»), en la primera de sus actuaciones («Administración orientada al ciudadano»), subapartado 4 («Nuevo modelo de identidad digital, que permita, entre otros, evolucionar e impulsar el Nodo eIDAS español»). Los hitos y objetivos que le son de aplicación son: Objetivo 161 («proyectos de transformación digital en términos de proactividad, movilidad y experiencia del usuario») e Hito 162 («Finalización de proyectos de apoyo a la transformación digital de la Administración General del Estado»).

La actual revisión del Reglamento eIDAS (el denominado eIDAS 2) establecerá un nuevo marco para una identidad digital europea, que ofrecerá a ciudadanos y empresas un medio armonizado de identificación electrónica que permitirá autenticar y compartir datos vinculados de su identidad ante las Administraciones Públicas y el sector privado. En este sentido, los Estados miembros ofrecerán a ciudadanos y empresas una «Cartera Digital» que proporcionará a las personas físicas y jurídicas de la Unión un medio de identificación electrónica armonizado que les permitirá autenticar y compartir datos vinculados a su identidad. Cada uno de los estados miembros notificará a la Comisión Europea su «Cartera digital» nacional que, en el caso de España, está siendo desarrollada por el Ministerio de Asuntos Económicos y Transformación Digital en ejecución de la mencionada medida 4 del Plan de Digitalización.

Por medio del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, se introdujo una disposición adicional sexta en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, según la cual y con relación a los sistemas de identificación y firma electrónicos previstos en los artículos 9.2 c) y 10.2 c) de dicha ley «no serán admisibles en ningún caso y, por lo tanto, no podrán ser autorizados, los sistemas de identificación basados en tecnologías de registro distribuido y los sistemas de firma basados en los anteriores, en tanto que no sean objeto de regulación específica por el Estado en el marco del Derecho de la Unión Europea».

No obstante, en el propio preámbulo del Real Decreto-ley 14/2019, de 31 de octubre, se matizaba que «las restricciones impuestas a los sistemas de identificaciones y firmas basados en tecnologías de registro distribuido en ningún caso suponen una prohibición general. Simplemente, se restringe puntualmente y de forma meramente provisional su uso como sistema de identificación y firma de los interesados cuando estos últimos se interrelacionan con la Administración y mientras no haya más datos o un marco regulatorio ad hoc de carácter estatal o europeo que haga frente a las debilidades que implica su uso para los datos y la seguridad pública».

En el marco nacional e internacional descrito, la necesidad de desarrollo y empleo de las nuevas tecnologías habilitadoras por parte de las Administraciones Públicas se está

acelerando, particularmente en lo tocante al uso de tecnologías de registro distribuido en sistemas de identificación a los usuarios debido a las grandes ventajas que ofrecen. De hecho, desde 2019 las tecnologías de registro distribuido se están implantando en determinados sectores, por ejemplo el financiero.

Por ello, para poder cumplir los compromisos adquiridos por España en el liderazgo de las propuestas señaladas sobre identidad digital y credenciales e infraestructura Blockchain que han sido seleccionadas por la Comisión Europea en el marco del programa Europa Digital, la limitación provisional de la Disposición adicional sexta en la Ley 39/2015, de 1 de octubre requiere una excepción específica para poder utilizar esta tecnología en el *wallet* en la ejecución de ambos proyectos y limitada a estos. Lo mismo ocurre con relación a la «Cartera digital» nacional que el Ministerio de Asuntos Económicos y Transformación Digital está desarrollando en ejecución de la mencionada medida 4 del Plan de Digitalización 2021-2025 y que dará cumplimiento a las previsiones del futuro Reglamento eIDAS 2.

Por último, cabe señalar que la instrumentación a través de Acuerdo de Consejo de Ministros se produce en cumplimiento del artículo 28 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, que regula los «Sistemas de clave concertada y otros sistemas de identificación de las personas interesadas», cuyo apartado 3, párrafo segundo, establece respecto de la creación de estos nuevos sistemas de identificación que cuando el nuevo sistema se refiera a la totalidad de la Administración General del Estado se requerirá Acuerdo del Consejo de Ministros a propuesta de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital.

En virtud de lo anteriormente expuesto, el Consejo de Ministros, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, en su reunión del día 27 de junio de 2023, acuerda:

Primero. *Validez de sistemas de identificación y firma electrónica cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido.*

1. De acuerdo con lo previsto en el artículo 28.3 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, y en aplicación de lo dispuesto en el apartado primero de la Disposición adicional sexta de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se podrá considerar válido un sistema de identificación y firma de los interesados por medio de una credencial incorporada a la Cartera digital cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido basado en la Infraestructura Europea de Servicios de Blockchain (EBSI, por sus siglas en inglés) en el contexto de los proyectos europeos vinculados a la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se modifica el Reglamento (UE) n.º 910/2014 en lo que respecta al establecimiento de un Marco para una Identidad Digital Europea (futuro Reglamento eIDAS 2) liderados por el Ministerio de Asuntos Económicos y Transformación Digital, que han seleccionados por la Comisión Europea en cumplimiento de la Decisión de Ejecución de la Comisión sobre la financiación del Programa Europa Digital y la adopción del plan plurianual programa de trabajo para 2021-2022 y el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 202, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240.

2. Asimismo, de acuerdo con lo previsto en el artículo 28.3 del Reglamento de actuación y funcionamiento del sector público por medios electrónicos y en aplicación de lo dispuesto en el mencionado apartado primero de la Disposición adicional sexta de la Ley 39/2015, de 1 de octubre, se podrá considerar válido un sistema de identificación y firma de los interesados por medio de una credencial cuya verificación se lleve a cabo por medio de un sistema de tecnología de registro distribuido incorporada a la Cartera digital española, para su utilización en los casos de uso del Consorcio europeo Digital Credentials For Europe (DC4EU) en el nuevo marco de identidad digital europea, que desarrolla el Ministerio de Asuntos Económicos y Transformación Digital en cumplimiento del Componente 11 del Plan de Recuperación Transformación y Resiliencia aprobado por Decisión del Consejo de 16 de junio de 2021 de acuerdo con el Reglamento (UE) 2021/241 del Parlamento Europeo y del

Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia y de la medida 4 del Eje Estratégico 1 («Transformación Digital de la Administración General del Estado») del Plan de Digitalización de las Administraciones Públicas 2021-2025, que establece un nuevo modelo de identidad digital cuyo objeto es desarrollar sistemas y servicios de identificación sencillos, seguros y usables por los ciudadanos.

3. En los casos previstos en los dos apartados anteriores la credencial o credenciales deberán ajustarse a lo previsto en el Esquema Nacional de Seguridad y contener, como mínimo, el nombre y apellidos y el número de Documento Nacional de Identidad, Número de Identificación de Extranjero o Número de Identificación Fiscal.

Segundo. *Autoridad intermedia.*

De acuerdo con lo previsto en el apartado segundo de la disposición adicional sexta de la Ley 39/2015, de 1 de octubre, la Administración General del Estado actuará como autoridad intermedia que ejercerá las funciones que corresponda para garantizar la seguridad pública con relación a los sistemas que se refiere este Acuerdo.

Tercero. *Entrada en vigor.*

Este Acuerdo surtirá efectos desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 20

Orden PCM/1382/2021, de 9 de diciembre, por la que se regula el Registro Electrónico General en el ámbito de la Administración General del Estado

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 296, de 11 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-20477

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente derogada, ya establecía en el artículo 24 que las Administraciones Públicas crearían registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones. Posteriormente, el Real Decreto 1671/2009, de 6 de noviembre, que desarrolló parcialmente esta ley, preveía la creación del Registro Electrónico Común de la Administración General del Estado que finalmente sería desarrollado por la Orden HAP/566/2013, de 8 de abril.

El artículo 16 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece que cada Administración dispondrá de un Registro Electrónico General en el que se hará el correspondiente asiento de todo documento que sea presentado o que se reciba en cualquier órgano administrativo, organismo público o entidad, vinculados o dependientes. También se podrá anotar la salida de los documentos oficiales dirigidos a otros órganos o particulares.

El precepto establece que los organismos públicos vinculados o dependientes de cada Administración podrán disponer de su propio registro electrónico plenamente interoperable e interconectado con el Registro Electrónico General de la Administración de la que depende.

Estos registros electrónicos contarán con el apoyo de las Oficinas de Asistencia en Materia de Registros a las que corresponde la digitalización y la anotación en el Registro Electrónico General, o registro electrónico de cada organismo o entidad según corresponda, de las solicitudes, escritos y comunicaciones en papel que se presenten o sean recibidos en estas y se dirijan a cualquier órgano, organismo público o entidad de derecho público de cualquier Administración Pública.

Para dar cumplimiento a estas previsiones legales, el artículo 38 del Reglamento de actuación y funcionamiento del Sector Público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, establece la naturaleza y funcionamiento del Registro Electrónico General de la Administración General del Estado.

De acuerdo con lo señalado anteriormente, se considera necesario regular los requisitos y condiciones del funcionamiento del Registro Electrónico General de la Administración General del Estado.

Esta orden se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En este sentido, la norma da cumplimiento a los principios de

necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. La misma persigue un interés general al pretender incrementar la eficiencia y la transparencia en el funcionamiento del sector público estatal. No existe ninguna alternativa regulatoria menos restrictiva, resulta coherente con el ordenamiento jurídico, no introduce nuevas cargas administrativas, y permite una gestión más eficiente de los recursos públicos.

Esta orden ha sido informada por la Agencia Española de Protección de Datos, en virtud del artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 5.3 b) del Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

En su virtud, a propuesta conjunta de la Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital y de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. La orden tiene por objeto regular los requisitos y condiciones del funcionamiento del Registro Electrónico General de la Administración General del Estado, (en adelante, REG-AGE).

2. De acuerdo con el artículo 38 del Reglamento de actuación y funcionamiento del Sector Publico por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, el REG-AGE se configura como el conjunto agregado de los asientos practicados a través de las aplicaciones de que dispongan las unidades que realicen anotaciones en registro, de las anotaciones que se realicen en cualquier aplicación que proporcione soporte a procedimientos específicos, así como de las anotaciones que se practiquen por medio del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible desde la sede electrónica del Punto de Acceso General de la Administración General del Estado.

3. El ámbito del REG-AGE es la Administración General del Estado y sus Organismos públicos y Entidades de derecho público vinculados o dependientes que no dispongan de su propio registro.

Artículo 2. *Órganos competentes.*

1. La Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública es competente para la gobernanza y gestión funcional del REG-AGE, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, implantación y gestión técnica de la plataforma tecnológica del REG-AGE y del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible desde la sede electrónica del Punto de Acceso General de la Administración General del Estado.

2. En cada Ministerio se designará una persona delegada del REG-AGE, con rango de Subdirector General o asimilado, pudiendo nombrar más de una persona delegada cuando el volumen de actividad o número de Oficinas de Asistencia en Materia de Registros así lo aconseje. La designación corresponderá al titular de la Subsecretaría o en su caso al Presidente o Director de sus organismos públicos y entidades de derecho público vinculados o dependientes.

La persona delegada será responsable del seguimiento del correcto funcionamiento del REG-AGE sobre los documentos que tengan como emisor o destinatario el ministerio y los organismos públicos y entidades de derecho público vinculados o dependientes y la coordinación de las Oficinas de Asistencia en Materia de Registros en relación con el REG-AGE.

Artículo 3. *Acceso al Registro Electrónico General de la Administración General del Estado.*

1. De acuerdo con lo previsto en el artículo 16 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se podrá acceder al REG-AGE a través de las siguientes vías:

a) Presencialmente, exclusivamente para los sujetos no obligados a relacionarse electrónicamente de acuerdo con el artículo 14 de la ley 39/2015, de 1 de octubre, a través de las Oficinas de Asistencia en Materia de Registros y en las representaciones diplomáticas u oficinas consulares de España en el extranjero. Asimismo, en las oficinas de Correos en los términos que se determinen reglamentariamente.

b) Por internet, a través de la sede electrónica del Punto de Acceso General de la Administración General del Estado (sede.administracion.gob.es) que dispondrá de un acceso al REG-AGE para la presentación de solicitudes, escritos y comunicaciones distintos de los mencionados en el apartado c).

c) Por internet, a través de las sedes electrónicas asociadas a los ministerios, organismos y entidades de derecho público de la Administración General del Estado para los servicios, procedimientos y aplicaciones de soporte que realicen anotaciones en el REG-AGE.

2. El Punto de Acceso General de la Administración General del Estado o su sede electrónica contendrá:

a) Información sobre las distintas vías de acceso al REG-AGE señaladas en el apartado 1.

b) Un enlace al servicio del REG-AGE accesible desde la sede electrónica del Punto de Acceso General de acuerdo con el apartado 1.b), junto con la descripción de los requisitos técnicos del servicio, el detalle del formulario general a utilizar para la presentación de solicitudes, escritos y comunicaciones y las especificaciones de la documentación que, en su caso, se acompañe.

c) Información actualizada de los servicios, procedimientos y trámites que cuenten con aplicaciones específicas que realicen anotaciones en el REG-AGE y un enlace a las sedes electrónicas a través de las cuales se acceda a los mismos.

Artículo 4. *Anotación en el Registro Electrónico General de la Administración General del Estado.*

1. Los asientos registrales en el REG-AGE se anotarán respetando el orden temporal de recepción o salida de los documentos, e indicarán la fecha y hora del día en que se produzcan. Concluido el trámite de registro en el REG-AGE, los documentos serán cursados sin dilación a sus destinatarios y a las unidades administrativas correspondientes desde el registro en que hubieran sido recibidas.

Los datos, formatos y protocolos así como la documentación para integradores se detallan en el Portal de la Administración Electrónica (PAe) en el siguiente enlace: https://administracionelectronica.gob.es/.

2. Se garantizará la constancia, en cada asiento que se practique, de un número, epígrafe expresivo de su naturaleza, fecha y hora de su presentación, identificación de la persona interesada, órgano administrativo remitente, si procede, y persona u órgano administrativo al que se envía, y, en su caso, referencia al contenido del documento que se registra.

Artículo 5. *Documentos admisibles a través del servicio electrónico accesible desde la sede electrónica del Punto de Acceso General.*

1. El servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible a través de la sede electrónica del Punto de Acceso General de la Administración General del Estado admitirá cualquier solicitud, escrito o comunicación relacionado con servicios, procedimientos y trámites que no cuenten con aplicaciones de soporte que realicen anotaciones en el REG-AGE.

2. El formulario general a utilizar para la presentación de solicitudes, escritos y comunicaciones a través de este acceso estará disponible en la propia sede electrónica del Punto de Acceso General de la Administración General del Estado.

3. Si fuera precisa la aportación de documentación complementaria que supere la extensión máxima a presentar en un solo registro electrónico se podrá llevar a cabo mediante una nueva presentación que incluirá, al menos, la referencia al número o código de

registro individualizado al que complementa o información suficiente que permita identificarlo.

Artículo 6. *Acuse de recibo.*

1. Independientemente del sistema de acceso al REG-AGE, se emitirá, automáticamente, un recibo firmado electrónicamente mediante alguno de los sistemas de firma previstos en el artículo 40 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con el siguiente contenido:

a) El número o código de registro individualizado.
b) La fecha y hora de presentación.
c) La copia autenticada del escrito, comunicación o solicitud presentada, siendo admisible a estos efectos la reproducción literal de los datos introducidos en el formulario de presentación.
d) En su caso, la enumeración y denominación de los documentos adjuntos al formulario de presentación o documento presentado, seguida de la huella electrónica de cada uno de ellos.

2. El citado recibo electrónico tendrá la consideración de acuse de recibo y su emisión no prejuzga la admisión definitiva del escrito de acuerdo con lo previsto en el artículo 16.8 de la Ley 39/2015, de 1 de octubre.

Artículo 7. *Consultas al REG-AGE.*

Desde el servicio electrónico de registro accesible desde la sede electrónica del Punto de Acceso General, el interesado podrá consultar sus asientos registrales realizados en el REG-AGE mediante dicho servicio, que contendrá, al menos:

a) El estado de las presentaciones.
b) El recibo de los asientos registrales.
c) Los documentos adjuntos correspondientes al asiento registral.

Artículo 8. *Presentación de documentos, fecha, hora oficial y cómputo de plazos.*

1. Cuando se acceda por internet al REG-AGE se permitirá la presentación de solicitudes, escritos y comunicaciones todos los días del año, durante las 24 horas del día, sin perjuicio de las interrupciones de mantenimiento técnico u operativo, que se anunciarán con la antelación que resulte posible y, en todo caso, con un mínimo de 24 horas en la sede electrónica del Punto de Acceso General de la Administración General del Estado junto con la ampliación concreta del plazo no vencido, según el artículo 32.4 de la Ley 39/2015, de 1 de octubre.

Cuando, por tratarse de interrupciones no planificadas que impidan la presentación de escritos, no resulte posible realizar su anuncio con antelación, se actuará conforme a lo establecido en el artículo 32.4 de la Ley 39/2015, de 1 de octubre, a cuyo efecto se podrá determinar una ampliación de los plazos no vencidos, debiendo publicarse en la sede electrónica tanto la incidencia técnica acontecida como la ampliación concreta del plazo no vencido.

Conforme a lo establecido en el artículo 31.2 de la Ley 39/2015, de 1 de octubre, la fecha y hora a computar en las anotaciones del REG-AGE será la oficial de la sede electrónica del Punto de Acceso General de la Administración General del Estado, debiendo adoptarse las medidas precisas para asegurar su integridad.

2. Para la presentación por internet a través de las sedes electrónicas asociadas de los ministerios, o las sedes electrónicas asociadas de los organismos públicos y entidades de derecho público de la Administración General del Estado para los servicios, procedimientos y trámites que cuenten con modelos normalizados de presentación y aplicaciones de soporte que realicen anotaciones en el REG-AGE, la fecha y hora a computar será la oficial de la correspondiente sede electrónica.

3. Para la presentación de documentos en las Oficinas de Asistencia en Materia de Registros se publicará en el Punto de Acceso General el listado de las oficinas y los días y el horario en el que permanecen abiertas.

4. El calendario de días inhábiles a efectos de cómputo de plazos en el REG-AGE será el que se determine en la resolución publicada cada año en el «Boletín Oficial del Estado» para todo el territorio nacional por el Ministerio de Hacienda y Función Pública, en cumplimiento del artículo 30.7 de la Ley 39/2015, de 1 de octubre.

Artículo 9. *Responsabilidad.*

Los usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos necesarios para su identificación en el acceso a los servicios prestados mediante administración electrónica, el establecimiento de la conexión precisa y la utilización de la firma electrónica, así como de las consecuencias que pudieran derivarse del uso indebido, incorrecto o negligente de los mismos.

Los departamentos ministeriales, entidades y organismos públicos destinatarios de los escritos presentados en el REG-AGE serán responsables de la custodia y manejo de los correspondientes ficheros, una vez se haya producido su entrega y recepción.

Artículo 10. *Protección de datos de carácter personal.*

De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando la persona interesada o su representante fueran personas físicas, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del REG-AGE se fundamenta en el artículo 6.1 c) y e) del citado Reglamento.

Previo análisis de los riesgos para los derechos y libertades de las personas físicas, se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

La Dirección General de Gobernanza Pública será la responsable del tratamiento, siendo la Secretaría General de Administración Digital la encargada del tratamiento según lo estipulado en el artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos.

Disposición adicional primera. *Integración en el REG-AGE.*

Los departamentos ministeriales, organismos públicos y entidades de derecho público vinculados o dependientes se coordinarán con la Secretaría General de Administración Digital para la integración de sus sistemas y plataformas de registro con el REG-AGE.

Las especificaciones técnicas, protocolos y formatos para la integración de sistemas y plataformas en el REG-AGE se publicarán en el Centro de Transferencia Tecnológica (CTT) del Portal de Administración Electrónica.

Disposición adicional segunda. *Comunicaciones entre Administraciones Públicas.*

Para los intercambios registrales entre Administraciones Públicas no será de utilización el servicio electrónico de registro accesible desde la sede electrónica del Punto de Acceso General. En su lugar, se podrán utilizar las aplicaciones o sistemas de información para el tratamiento del Registro Electrónico General de cada Administración así como del registro electrónico de cada organismo público o entidad de derecho público vinculado o dependiente, a través del sistema de interconexión de registros (SIR).

El REG-AGE dispondrá de un modelo único de numeración para su empleo en el registro de los asientos por parte de todas las unidades.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden HAP/566/2013, de 8 de abril, por la que se regula el Registro Electrónico Común, y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta orden.

Disposición final única. *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 21

Orden PCM/1383/2021, de 9 de diciembre, por la que se regula el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado, sus Organismos Públicos y Entidades de Derecho Público

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 296, de 11 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-20478

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, consagraba el derecho de la ciudadanía a relacionarse con las Administraciones Públicas por medios electrónicos. Para ello era necesario no solo incorporar las nuevas tecnologías a su funcionamiento interno sino, al mismo tiempo, garantizar a aquellas personas interesadas, que por cualquier motivo no pudiesen acceder electrónicamente a la Administración Pública, disponer de medios adecuados para comunicarse con ella con los mismos derechos y garantías.

El artículo 22 de esa ley preveía que, en aquellos supuestos en los que para la realización de cualquier operación por medios electrónicos se requiriese la identificación o autenticación de la persona interesada mediante algún instrumento de los previstos en el artículo 13, y la persona no dispusiese de ellos, la identificación o autenticación podría ser válidamente realizada por el personal funcionario mediante el uso del sistema de firma electrónica del que estuvieran dotados.

El Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, concretaba en su artículo 16 esta habilitación, especificando que para la identificación y autenticación de las personas interesadas por el personal funcionario público, en los servicios y procedimientos en los que resultase necesaria la utilización de sistemas de firma electrónica de los que careciesen, la persona funcionaria habilitada debería disponer de un sistema de firma electrónica admitido por el órgano u organismo público destinatario de la actuación.

La Orden HAP/7/2014, de 8 de enero, del Registro de Funcionarios Habilitados para la identificación y autenticación de ciudadanos, en el ámbito de la Administración General del Estado y sus Organismos públicos vinculados o dependientes, estableció por primera vez la regulación de un registro del personal de funcionario que pudieran asistir a las personas interesadas en la realización de determinados trámites electrónicos de identificación y autenticación en su nombre.

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recoge y amplía esta figura. Así, en línea con la normativa anterior, se establece en su artículo 12 que cuando las personas interesadas, que no estén obligadas a relacionarse electrónicamente con las Administraciones Públicas, no dispongan

de los medios electrónicos necesarios, su identificación o firma electrónica en el procedimiento administrativo podrá ser válidamente realizada por el personal funcionario público mediante el uso del sistema de firma electrónica del que esté dotado para ello.

A estos efectos, se prevé que la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales mantengan actualizado un registro u otro sistema equivalente, donde constará el personal funcionario habilitado para la identificación o firma y en el que se incluirán, al menos, aquellos que presten servicios en las Oficinas de Asistencia en Materia de Registros.

Por otra parte, el artículo 27 de la Ley 39/2015, de 1 de octubre, al regular la validez y eficacia de las copias realizadas por las Administraciones Públicas, prevé que la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales podrán realizar copias auténticas mediante personal funcionario habilitado o mediante actuación administrativa automatizada para lo que deberán mantener actualizado un registro u otro sistema equivalente, donde constará el personal funcionario habilitado para la expedición de copias auténticas. En este artículo también se precisa que en el mismo constará, al menos, el personal funcionario que preste servicios en las Oficinas de Asistencia en Materia de Registros.

La exposición de motivos de la citada ley establece que, si así decide, cada Administración podrá hacer constar en este registro o sistema equivalente conjuntamente el personal funcionario dedicado a asistir a las personas interesadas en el uso de medios electrónicos y el facultado para realizar copias auténticas, no existiendo impedimento a que una misma persona funcionaria tenga reconocida ambas funciones o solo una de ellas.

El Reglamento de actuación y funcionamiento del Sector Publico por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, crea en su artículo 31 el Registro de Funcionarios Habilitados en el ámbito de la Administración General del Estado y sus Organismos públicos y Entidades de derecho público, previendo en su apartado cuarto que la regulación de su funcionamiento se realizará por orden conjunta de las personas titulares del Ministerio de Hacienda y Función Pública y del Ministerio de Asuntos Económicos y Transformación Digital. Además, señala en el segundo apartado que el registro será interoperable con los sistemas equivalentes que ya existan en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho público vinculados o dependientes.

Conforme a este marco legal y reglamentario, esta orden tiene por objeto regular el funcionamiento del Registro de Funcionarios Habilitados para la expedición de copias auténticas y para la identificación o firma electrónica de las personas interesadas en aquellos procedimientos que se determinen y que estarán disponibles para la ciudadanía en el Punto de Acceso General de la Administración General del Estado.

Esta orden se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En este sentido, la norma da cumplimiento a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. Además, persigue un interés general al pretender incrementar la eficiencia, y la transparencia en el funcionamiento del sector público estatal. No existe ninguna alternativa regulatoria menos restrictiva, resulta coherente con el ordenamiento jurídico y permite una gestión más eficiente de los recursos públicos.

La norma ha sido informada por la Agencia Española de Protección de Datos, en virtud del artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 5.3 b) del Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

En su virtud, a propuesta conjunta de la Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital y de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

De acuerdo con lo previsto en el artículo 31.4 del Reglamento de actuación y funcionamiento del Sector Publico por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, esta orden tiene por objeto la regulación del Registro de

Funcionarios Habilitados, (en adelante, RFH), en el ámbito de la Administración General del Estado y sus organismos públicos y entidades de derecho públicos vinculados o dependientes.

Artículo 2. *Órganos competentes.*

1. La Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública asume la gobernanza y gestión del RFH, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, la implantación y la gestión técnica de la plataforma tecnológica que soporte el Registro.

2. La inscripción del personal funcionario que se relaciona en el artículo 3.1 de esta orden corresponde a los titulares de los órganos y unidades donde estos presten servicios.

3. Producida la anotación de la habilitación del personal funcionario, el registro generará una credencial en la que se hará constar su identificación personal y administrativa, los procedimientos y servicios a los que alcanza su habilitación, la fecha de inicio de la misma y, en su caso, su fecha de fin.

Artículo 3. *Inscripción en el registro.*

1. En el RFH, regulado por esta orden, deberán inscribirse:

a) El personal funcionario habilitado para realizar la identificación o firma electrónica de las personas interesadas no obligadas a relacionarse electrónicamente con la Administración, conforme a lo previsto en el artículo 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en aquellos procedimientos que se determinen por el ministerio, organismo o entidad competente para su tramitación.

b) El personal funcionario habilitado para la expedición de copias auténticas de los documentos públicos administrativos o privados, ya sea en formato papel o electrónico, conforme a lo previsto en el artículo 27 de la Ley 39/2015, de 1 de octubre.

c) El personal funcionario habilitado que presta servicios en las Oficinas de Asistencia en Materia de Registros, que estará habilitado para la identificación o firma electrónica de las personas interesadas en aquéllos procedimientos y servicios que se determinen y para la expedición de copias auténticas electrónicas de cualquier documento en papel que presenten las personas interesadas para que se remitan desde la citada oficina a la unidad competente para su incorporación a un expediente administrativo.

2. Podrán ser habilitados tanto el personal funcionario de carrera como interino, en servicio activo, a que se refiere el artículo 8.2 a) y b) del Texto Refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y presten servicios en la Administración General del Estado o en cualquiera de sus organismos públicos o entidades de derecho público vinculados o dependientes.

Artículo 4. *Identificación y firma electrónica.*

1. La persona interesada, previa acreditación de su identidad, deberá dar su consentimiento expreso para su identificación o firma por el personal funcionario habilitado para cada actuación administrativa que la requiera, a través del formulario que se incluye como Anexo I disponible en el Punto de Acceso General electrónico de la Administración General del Estado (https://administracion.gob.es).

2. El personal funcionario habilitado entregará a la persona interesada toda la documentación acreditativa del trámite realizado así como una copia del documento de consentimiento expreso cumplimentado y firmado. A estos efectos, el personal funcionario habilitado utilizará el sistema de firma electrónica del que esté dotado para ello.

Artículo 5. *Expedición de copias auténticas.*

1. La habilitación para la expedición de copias auténticas, a la que se refiere el artículo 3.1 b), será conferida por los titulares de los órganos a los que corresponda la emisión de los

documentos originales, su custodia, el archivo de documentos o que en sus normas de competencia así se haya previsto.

2. El personal funcionario que preste servicios en las Oficinas de Asistencia en Materia de Registros está habilitado para la expedición de copias auténticas electrónicas de cualquier documento en papel que presenten las personas interesadas para que se remita desde la citada oficina a la unidad competente para su incorporación a un expediente administrativo.

Artículo 6. *Contenido del Registro de Funcionarios Habilitados.*

En el RFH constarán los siguientes datos del personal funcionario habilitado:

a) Documento Nacional de Identidad.
b) Nombre y apellidos.
c) Órgano, organismo o entidad en el que presta servicios, centro directivo y centro de destino identificados mediante su código asignado en el Directorio Común de Unidades Orgánicas y Oficinas, indicándose el código de oficina para el caso de personal funcionario destinado en una Oficina de Asistencia en Materia de Registros.
d) Puesto de trabajo que desempeña.
e) Correo electrónico corporativo
f) Fecha de alta en el RFH.
g) Tipo de habilitaciones: identificación o firma electrónica y/o expedición de copias auténticas.
h) Procedimientos y servicios para los que se tiene autorizada la habilitación, identificados mediante su código asignado en el inventario del Sistema de Información Administrativa.
i) Fecha de baja en el RFH.
j) Causas de las cancelaciones de las habilitaciones.

Artículo 7. *Funcionamiento del Registro de Funcionarios Habilitados.*

1. La inscripción como personal funcionario habilitado en el RFH tendrá una duración máxima de cinco años prorrogable de forma expresa por periodos quinquenales sucesivos.

2. La habilitación continuará vigente durante el periodo previsto en el apartado anterior en tanto no se supriman los procedimientos y servicios a los que alcanza su habilitación, o en tanto no se produzca un cambio de puesto de trabajo. Asimismo, la habilitación podrá ser revocada en cualquier momento por el órgano competente para su concesión.

3. Se podrá consultar la base de datos del Registro Central de Personal o sistema equivalente únicamente a efectos de la comprobación de los datos de la situación administrativa y del destino del personal funcionario habilitado.

4. La inscripción de la habilitación continuará vigente hasta que se cancele la misma en el RFH, en los supuestos contemplados en el apartado segundo, o hasta que transcurra el periodo máximo de vigencia sin prórroga expresa.

5. En el Sistema de Información Administrativa deberán constar los procedimientos y servicios para los que pueda conferirse la habilitación incorporada al RFH según determine el órgano responsable de los mismos. La supresión de algún procedimiento o servicio en dicho inventario impedirá su gestión por medio de personal funcionario habilitado y provocará la cancelación de las habilitaciones ligadas al mismo.

6. Se utilizarán los códigos de los procedimientos y servicios administrativos asignados en el inventario del Sistema de Información Administrativa de la Administración General del Estado previsto en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración electrónica.

Artículo 8. *Publicidad de procedimientos.*

En el Punto de Acceso General de la Administración General del Estado se publicará una relación de todos los procedimientos y servicios por medios electrónicos que se determinen expresamente por los departamentos ministeriales, organismos públicos o entidades de derecho público vinculados o dependientes que han sido objeto de habilitación. Respecto a cada uno de los procedimientos y servicios que figuren en dicha relación se hará

constar su descripción, código identificativo y las Oficinas de Asistencia en Materia de Registros u otras dependencias de atención al ciudadano en las que los ciudadanos puedan ejercer el derecho.

Artículo 9. *Acceso electrónico al Registro de Funcionarios Habilitados por las Administraciones Públicas.*

1. El RFH será accesible para los órganos de cualquier Administración Pública, sus organismos públicos y entidades de derecho público para obtener información sobre habilitaciones.

2. El registro ofrecerá a los órganos y organismos interesados, como vía de acceso a la información, el acceso en línea mediante servicios web a los efectos de comprobar, automáticamente y en tiempo real desde las aplicaciones, la habilitación de un funcionario para el procedimiento al que den soporte. Las peticiones al registro para los procedimientos y trámites por medios electrónicos, de las que el órgano u organismo administrativo peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello electrónico cualificado del citado órgano o administración de adscripción. La aplicación de soporte al registro mantendrá trazabilidad de todas las peticiones recibidas.

Artículo 10. *Protección de Datos de Carácter Personal.*

De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del RFH se fundamenta en el artículo 6.1 b), c) y d) del citado Reglamento.

Previo análisis de los riesgos para los derechos y libertades de las personas físicas se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario. Las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad, deberían prevalecer sobre éstas últimas a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

Se adoptarán las medidas que se estimen adecuadas para garantizar que la cancelación de las inscripciones y, en su caso, la rectificación de los datos personales, se realizarán sin dilación teniendo en cuenta que se trata de datos personales correspondientes a funcionarios públicos que se encuentran en poder de la Administración.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Orden HAP/7/2014, de 8 de enero, por la que se regula el Registro de Funcionarios Habilitados para la identificación y autenticación de ciudadanos en el ámbito de la Administración General del Estado y sus Organismos públicos vinculados o dependientes.

Disposición final primera. *Modificación de formularios.*

Corresponde a la persona titular de la Secretaría de Estado de Función Pública la actualización de los formularios previstos en los Anexos I y II de esta orden relativos al consentimiento por parte de la persona interesada para su identificación o firma por la persona funcionaria habilitada, y a la habilitación conferida al personal funcionario, así como la aprobación de otros formularios que, en su caso, resulten precisos para la gestión de dicho Registro.

Estos formularios serán publicados en el Punto de Acceso General de la Administración General del Estado (https://administracion.gob.es).

Disposición final segunda. *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Consentimiento expreso del/la interesado/a para su identificación, y en su caso firma electrónica por /habilitado.

D./D.ª .....

DNI: .....

DECLARA:

QUE NO DISPONE DE LOS MEDIOS ELECTRÓNICOS NECESARIOS PARA SU IDENTIFICACIÓN Y/O FIRMA Y QUE OTORGA SU CONSENTIMIENTO, POR ESTA ÚNICA VEZ, PARA LA IDENTIFICACIÓN O FIRMA POR EL/LA FUNCIONARIO/A HABILITADO/A ABAJO FIRMANTE, PARA LA REALIZACIÓN DEL SIGUIENTE TRÁMITE O ACTUACIÓN ELECTRÓNICA:

- DESCRIPCIÓN DEL TRÁMITE O ACTUACIÓN:
- CÓDIGO SIA[1]:

---

[1] A cumplimentar por la Administración.

EL/LA FUNCIONARIO/A CON IDENTIFICACIÓN:

NOMBRE Y APELLIDOS: ……

N.º DE CREDENCIAL: ……

En ..... a ..... de ..... de .....

EL/LA INTERESADO/A EL/LA FUNCIONARIO/A HABILITADO/A

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS en cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Responsable del tratamiento: Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública, con domicilio en la calle Manuel Cortina 2, 28010 Madrid.

Encargado del tratamiento: Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital.

Finalidad: acreditar el consentimiento expreso del ciudadano a la habilitación del funcionario en los términos fijados por el Art. 12 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Legitimación: cumplimiento de una obligación legal (artículo 6.1 e) RGPD.

Destinatarios: Persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO I

Para la cumplimentación y tramitación del consentimiento expreso del/la interesado/a para su identificación y autenticación por personal funcionario público habilitado, se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada actuación electrónica que el/ la interesado/a desee realizar a través del personal funcionario habilitado, consignando, en cada caso, todos los datos que se requieren en el modelo de formulario.

b) En el caso de que se realicen varias acciones sobre un mismo procedimiento, se cumplimentarán tantos ejemplares como acciones se vayan a realizar.

c) Al efectuar la actuación, el personal funcionario habilitado presentará a el/la interesado/a copia impresa de la cumplimentación de datos en el sistema de información que dé soporte al mismo, para que éste dé su conformidad, mediante su firma en el impreso, antes de proceder a completar la actuación.

d) El personal funcionario habilitado entregará al/la interesado/a una copia del documento cumplimentado y firmado por ambas partes.

ANEXO II

Modelo normalizado para la habilitación de los/las funcionarios/as

D./D.ª .....

DNI .....

TITULAR DE (ÓRGANO COMPETENTE PARA OTORGAR LAS HABILITACIONES)

……

ACREDITO A:

D./D.ª ……

DNI ……

Correo electrónico corporativo ……

Funcionario/a del Cuerpo ……

Con destino en Ministerio ……

Centro Directivo/Organismo ……

Centro de destino/Oficina ……

Puesto de trabajo ……

☐ Como funcionario/a habilitado/a para la identificación y firma de los/las interesados/as en los procedimientos que se indican a continuación:

Descripción del procedimiento y código SIA

…

☐ Como funcionario/a habilitado/a para la expedición de copias auténticas de los documentos públicos administrativos válidamente emitidos por las Administraciones Públicas:

Descripción del procedimiento y código SIA

…

☐ Como funcionario/a habilitado/a para la expedición de copias electrónicas auténticas de los documentos que presenten los/las interesados/as y se vayan a incorporar a un expediente.

§ 22

Orden PCM/1384/2021, de 9 de diciembre, por la que se regula el Registro Electrónico de apoderamientos en el ámbito de la Administración General del Estado

Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática
«BOE» núm. 296, de 11 de diciembre de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-20479

El Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, regula en su artículo 33 el Registro Electrónico de Apoderamientos de la Administración General de Estado y establece en su apartado 4 que mediante orden conjunta de la persona titular del Ministerio de Hacienda y Función Pública y de la persona titular del Ministerio de Asuntos Económicos y Transformación Digital se regularán los requisitos y condiciones de funcionamiento del mismo.

La creación del Registro Electrónico de Apoderamientos de la Administración General de Estado tiene como finalidad facilitar la acreditación de la representación de las personas interesadas en procedimientos administrativos en los que tengan o puedan tener la condición de persona interesada, previa realización voluntaria de un apoderamiento por comparecencia personal o electrónica apud acta a favor de otra persona para que realice trámites en su nombre, sin coste alguno.

Mediante esta orden se determinan los órganos responsables y el sistema de funcionamiento en el ámbito de la Administración General del Estado, el procedimiento de incorporación de los apoderamientos, así como la revocación, renuncia, vigencia y prórroga de los apoderamientos.

Por otra parte, se aprueban los modelos de poderes inscribibles en el ámbito de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con registro electrónico de apoderamientos propio.

Esta orden se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre. En este sentido, la norma da cumplimiento a los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia. La misma persigue un interés general al pretender incrementar la eficiencia, y la transparencia en el funcionamiento del sector público estatal. No existe ninguna alternativa regulatoria menos restrictiva, resulta coherente con el ordenamiento jurídico, y permite una gestión más eficiente de los recursos públicos.

Esta orden ha sido informada por la Agencia Española de Protección de Datos, en virtud del artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y del artículo 5.3.b) del Estatuto de la

Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio.

En su virtud, a propuesta conjunta de la Vicepresidenta Primera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital y de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Esta orden tiene por objeto regular los requisitos y condiciones de funcionamiento del Registro Electrónico de Apoderamientos de la Administración General del Estado (en adelante, REA-AGE) en el ámbito de la Administración General del Estado y de sus organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con un registro electrónico de apoderamientos particular.

2. El REA-AGE será accesible desde la sede electrónica del Punto de Acceso General de la Administración General del Estado así como desde las sedes electrónicas asociadas de la Administración General del Estado y las sedes electrónicas o sedes electrónicas asociadas de los organismos públicos o entidades de derecho público vinculados o dependientes.

3. En el REA-AGE se inscribirán los apoderamientos a los que se refiere el artículo 3 otorgados apud acta a favor de la persona representante, presencial o electrónicamente, por quien pueda tener la condición de persona interesada en un procedimiento administrativo.

4. Asimismo esta orden tiene por objeto aprobar los modelos que figuran en los anexos I a V en los que se concretan los actos objeto de inscripción en el REA-AGE que podrán consistir en la inscripción del otorgamiento de poder apud acta; revocación por el poderdante, prórroga de la vigencia del poder, aceptación de la persona apoderada y renuncia del poder por la persona apoderada.

Los modelos se utilizarán para su presentación en papel mediante comparecencia personal en las Oficinas de Asistencia en Materia de Registros de la Administración General del Estado, por personas físicas no obligadas a relacionarse con la Administración por medios electrónicos.

Artículo 2. *Órganos competentes.*

1. La Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública asume la gobernanza y gestión funcional del REA-AGE, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, implantación y gestión técnica de la plataforma tecnológica que soporte el registro.

2. En cada ministerio se designará una persona delegada del REA-AGE con rango Subdirector General o asimilado, que desempeñará las funciones previstas en el artículo 6 de esta orden. Se podrá nombrar más de una persona delegada cuando el volumen de actividad o número de Oficinas de Asistencia en Materia de Registros así lo aconseje.

La designación corresponderá a la persona titular de la Subsecretaría o, en su caso, a la persona titular de la Presidencia o de la Dirección del organismo público o entidad de derecho público correspondiente.

Artículo 3. *Tipos de apoderamientos y contenido del REA-AGE.*

1. Los poderes que se inscriban en el REA-AGE corresponderán a alguno de los siguientes tipos:

a) Poder general para que la persona apoderada pueda actuar en nombre de la poderdante en cualquier actuación administrativa y ante cualquier Administración Pública, incluidos los organismos públicos o entidades de derecho púbico que cuenten con registro electrónico de apoderamientos particular, conforme a lo previsto en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

b) Poder para que la persona apoderada pueda actuar en nombre de la poderdante en cualquier actuación administrativa ante la Administración General del Estado y/o sus organismos públicos o entidades de derecho público vinculados o dependientes concretos

que no cuenten con registro electrónico de apoderamientos particular, conforme a lo previsto en el artículo 6.4.b) de la Ley 39/2015, de 1 de octubre.

c) Poder, para que la persona apoderada pueda actuar en nombre de la persona poderdante para la realización de determinados trámites especificados en el poder, ante un órgano de la Administración General del Estado o ante un organismo público o entidad de derecho público vinculado o dependiente de la misma que no cuente con registro de apoderamientos particular, conforme a lo previsto en el artículo 6.4.c) de la Ley 39/2015, de 1 de octubre.

2. Cada departamento ministerial u organismo público o entidad de derecho público vinculado o dependiente indicará en el Sistema de Información Administrativa, regulado en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, los trámites que pueden ser objeto de apoderamiento a través del poder previsto en el apartado 1.c).

En la sede electrónica del PAGe (https://sede.administracion.gob.es) figurará una relación pública de dichos trámites.

3. El apoderamiento podrá ser otorgado por varias personas físicas a una persona apoderada que tenga condición de persona física o jurídica.

4. Para inscribir un apoderamiento en el REA-AGE, se hará constar:

a) Nombre y apellidos (para el caso de persona física), denominación o razón social (para el caso de persona jurídica) y Documento Nacional de Identidad, Número de Identificación Fiscal o Número de Identidad de Extranjero de la persona o entidad poderdante.

b) Nombre y apellidos (para el caso de persona física), denominación o razón social (para el caso de persona jurídica) y Documento Nacional de Identidad, Número de Identificación Fiscal o Número de Identidad de Extranjero de la persona apoderada.

c) Tipología del poder.

d) Periodo de vigencia del poder.

e) Fecha de otorgamiento.

f) Número de referencia del alta y fecha de alta en el REA-AGE.

g) Copia del poder otorgado en documento público o privado con firma electrónica o notarialmente legitimada cuando la inscripción se realice a solicitud de la persona apoderada. En este caso constará también su bastanteo, sin perjuicio de la apreciación concreta por los órganos instructores del procedimiento, de su suficiencia en la actuación o procedimiento en que se emplee.

h) Declaración responsable que acredite que se contempla la posibilidad de representar a terceros ante las Administraciones Públicas en los Estatutos de la persona jurídica cuando actúe como persona apoderada.

Artículo 4. *Inscripción de los apoderamientos en el REA-AGE.*

1. Cuando la persona poderdante sea persona física no obligada a relacionarse electrónicamente con las Administraciones Públicas, el apoderamiento y su posterior solicitud de inscripción en el REA-AGE podrá realizarlo apud acta mediante su comparecencia personal en una Oficina de Asistencia en Materia de Registros de la Administración General del Estado.

También lo podrá realizar electrónicamente apud acta, en el REA-AGE, mediante el uso de los sistemas de identificación y firma electrónica previstos en los artículos 9 y 10 de la Ley 39/2015 de 1 de octubre.

2. Cuando de acuerdo a lo dispuesto en el artículo 14 de la Ley 39/2015, de 1 de octubre, la persona poderdante se relacione obligatoria o voluntariamente con las Administraciones Públicas por medios electrónicos, la solicitud de inscripción del apoderamiento solo podrá llevarse a cabo electrónicamente, utilizando los medios de identificación y firma electrónica previstos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre.

En el caso de que la persona poderdante realice la solicitud de inscripción en el REA-AGE en su condición de representante de una persona jurídica, los medios electrónicos

utilizados por aquella permitirán acreditar la representación y capacidad alegadas para realizar las actuaciones ante el mismo.

3. La solicitud de inscripción se presentará en el modelo del anexo I de esta orden en el caso de comparecencia personal, o en el formulario electrónico basado en el anterior cuando se acceda por internet.

La solicitud de inscripción quedará anotada automáticamente en el Registro Electrónico General para constancia de la presentación por la persona interesada.

Si la persona apoderada es persona jurídica se procederá a la inscripción cuando conste la documentación a la que se refiere el artículo 3.4.h).

La inscripción en el REA-AGE solicitada por el poderdante será efectiva en el momento en el que quede inscrita la aceptación por la persona apoderada y haya sido incorporado el bastanteo del poder cuando este sea jurídicamente exigible.

4. La inscripción de apoderamientos en el REA-AGE puede realizarse también a solicitud de la persona apoderada, exigiéndose en este supuesto que aporte una copia o certificación del poder otorgado mediante documento público o privado con firma electrónica o notarialmente legitimada. En el caso de aportar poderes notariales se exigirá un Código Seguro de Verificación (CSV en adelante), para poder acceder al sistema de consulta y conocer el contenido y la situación de vigencia del mismo. Si no se dispone de un CSV, se consignarán los datos identificativos del documento notarial.

Cuando el poder se haya otorgado en documento privado con firma electrónica, la solicitud de inscripción por la persona apoderada solo se podrá presentar por medios electrónicos.

Artículo 5. *Aceptación por la persona apoderada.*

1. El poder no surtirá efectos en tanto no se inscriba en el REA-AGE la aceptación de la persona apoderada. Se entenderá la aceptación tácita en el caso de que la solicitud de inscripción la presente la persona apoderada.

2. La aceptación por la persona apoderada se acreditará, surtiendo efectos inmediatos, por cualquiera de los siguientes medios:

a) Por comparecencia personal de la persona física apoderada no obligada a relacionarse con la administración por medios electrónicos. Presentará el modelo del anexo IV en una Oficina de Asistencia en Materia de Registros y el personal funcionario de la oficina entregará un justificante de la presentación a la persona interesada, quedando anotado automáticamente en el Registro Electrónico General.

b) Electrónicamente, mediante el formulario basado en el anexo IV, utilizando los sistemas de identificación y firma electrónica previstos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, y en el caso de representante de persona jurídica utilizará los medios electrónicos que permitan acreditar la representación y capacidad de actuación necesarios. La aceptación quedará anotada automáticamente en el Registro Electrónico General para constancia de la presentación para la persona interesada.

3. El plazo máximo de aceptación por parte de la persona apoderada no podrá superar los veinte días hábiles desde la fecha de alta de la solicitud de inscripción en el REA-AGE. Transcurrido este periodo, se entenderá que no ha aceptado el apoderamiento.

Artículo 6. *Comprobación del contenido del apoderamiento y bastanteo.*

1. Para poder inscribir válidamente un apoderamiento en el REA-AGE la solicitud deberá cumplir todos los requisitos establecidos en el artículo 3.

2. Además, con carácter previo a la inscripción, se realizarán las siguientes comprobaciones:

a) En los apoderamientos cuya inscripción se solicite electrónicamente, la aplicación informática del REA-AGE únicamente permitirá inscribir una solicitud basada en el anexo I que contenga todos los datos requeridos, que vaya acompañada de los documentos que, en su caso, sean preceptivos y se hayan cumplido los requisitos de identificación y firma electrónicas. En aquellos casos en los que se detecten anomalías de tipo técnico, el sistema lo pondrá en conocimiento de la persona interesada a los efectos oportunos.

b) En los apoderamientos otorgados mediante comparecencia personal, el personal funcionario de la Oficina de Asistencia en Materia de Registros de la Administración General del Estado verificará la identidad de la persona compareciente, que el modelo del anexo I está debidamente cumplimentado en todos los apartados aplicables al tipo de apoderamiento de que se trate, así como que se aporta la documentación complementaria que, en su caso, sea necesaria. Se hará constar la identificación de la persona funcionaria ante quien comparece para dar de alta en el REA-AGE los apoderamientos.

3. Cuando la persona apoderada aporte documento público o privado con firma electrónica o notarialmente legitimada, será necesario el bastanteo de los poderes, que se solicitará de la siguiente manera:

a) Cuando se trate de la solicitud de inscripción de un apoderamiento general ante cualquier Administración Pública previsto en el artículo 3.1.a) o de un apoderamiento previsto en el artículo 3.1.b) para actuar ante la Administración General del Estado y todos sus organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con Registro electrónico de apoderamientos particular la Dirección General de Gobernanza Pública del Ministerio de Hacienda y Función Pública será la responsable de solicitar el bastanteo de los poderes a su servicio jurídico, en los términos que al efecto establezca la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado.

El eventual requerimiento de subsanación de defectos en la representación a la persona interesada, será llevado a cabo por la Dirección General de Gobernanza Pública, concediendo un plazo de diez días hábiles para que se subsane la falta o acompañe los documentos preceptivos con indicación de que, si así no lo hiciera, se le tendrá por desistido de su solicitud de inscripción, previa resolución que deberá ser dictada en los términos previstos en los artículos 21 y 68 de la Ley 39/2015, de 1 de octubre.

b) Cuando se trate de la solicitud de inscripción de un apoderamiento previsto en el artículo 3.1.b) o en el artículo 3.1.c), para actuar ante un organismo público o entidad de derecho público concreto vinculado o dependiente de la Administración General del Estado que no cuente con registro electrónico de apoderamientos propio, o de la inscripción de un apoderamiento previsto en el párrafo c) del artículo 3.1 para actuar ante un ministerio, organismo o entidad concreto que no cuente con registro electrónico de apoderamientos propio, se procederá en la forma señalada en el apartado anterior, siendo la persona delegada del REA-AGE del ministerio, organismo o entidad al que esté adscrito el órgano competente de los trámites objeto del apoderamiento, el responsable de solicitar el bastanteo de los poderes al servicio jurídico correspondiente, en los términos que al efecto establezca la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado y, en su caso, requerir la subsanación de defectos.

Artículo 7. *Revocación y renuncia del apoderamiento.*

1. La inscripción de la revocación por la persona poderdante o de la renuncia por la persona apoderada de un apoderamiento inscrito en el REA-AGE se acreditará aportando los modelos previstos en los anexos II y III, respectivamente, o sus equivalentes electrónicos, surtiendo efecto en ambos casos desde la fecha de su inscripción.

2. La solicitud de inscripción en el REA-AGE se llevará a cabo en la misma forma prevista en el artículo 5.2 para la aceptación de un poder.

Artículo 8. *Vigencia y prórroga del apoderamiento.*

1. El apoderamiento tendrá una vigencia máxima de cinco años a contar desde la fecha de su inscripción en el REA-AGE.

2. En cualquier momento antes de la finalización del plazo de vigencia la persona poderdante podrá prorrogarlo y solicitar la inscripción de dicha prórroga, utilizando para ello el modelo previsto en el anexo V o su equivalente electrónico, según corresponda, y por los mismos medios previstos en el artículo 5.2.

3. Las prórrogas tendrán una vigencia máxima de cinco años a contar desde la fecha su inscripción en el REA-AGE.

Artículo 9. *Consultas por la persona interesada.*

El REA-AGE no tiene carácter público por lo que solo la persona interesada, una vez identificada, podrá consultar el REA-AGE electrónica o presencialmente, según corresponda, y acceder a la información de los apoderamientos de los que sea poderdante o apoderada.

Artículo 10. *Consultas por los órganos de la Administración General del Estado, organismos públicos o entidades de derecho público vinculados o dependientes.*

1. El REA-AGE permitirá la consulta de los órganos, organismos públicos y entidades de derecho público interesados a los efectos de comprobar que un apoderamiento está vigente.

2. Las peticiones de consulta al REA-AGE, relativas a los apoderamientos vigentes y válidos para los procedimientos por medios electrónicos de las que el órgano administrativo peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello electrónico cualificado del citado órgano o administración de adscripción. La aplicación de soporte mantendrá trazabilidad de todas las peticiones recibidas.

3. Las consultas se limitarán a los datos estrictamente necesarios para verificar la existencia, vigencia y alcance de los poderes en relación con las concretas actuaciones administrativas que se pretenden realizar y para poder comunicarse con la persona representante.

Artículo 11. *Protección de Datos de Carácter Personal.*

1. De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando la persona poderdante o la apoderada tuvieran condición de personas físicas, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del REA-AGE se fundamenta en el artículo 6.1.e) del reglamento.

2. Previo análisis de los riesgos para los derechos y libertades de las personas físicas, se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Las medidas a implantar como consecuencia del análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre estas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de protección de datos.

3. La Dirección General de Gobernanza Pública será la responsable del tratamiento, siendo la Secretaría General de Administración Digital la encargada del tratamiento según lo estipulado en el artículo 28 del Reglamento general de protección de datos.

Artículo 12. *Interoperabilidad del Registro.*

El REA-AGE deberá ser plenamente interoperable con los registros electrónicos de apoderamientos generales y particulares pertenecientes a todas y cada una de las administraciones garantizando su interconexión, compatibilidad informática, así como la transmisión electrónica de las solicitudes, escritos y comunicaciones que se incorporen al mismo, de acuerdo con lo previsto en el artículo 6.2 de la Ley 39/2015, de 1 de octubre.

Disposición adicional primera. *Entidades sin personalidad jurídica.*

Las previsiones que se contienen en esta orden sobre las personas jurídicas serán aplicables, a las entidades sin personalidad jurídica, que solo podrán actuar como poderdantes.

Disposición adicional segunda. *Actualización de modelos normalizados.*

Corresponde a la persona titular de la Secretaría de Estado de Función Pública, la actualización de los formularios previstos en los anexos I, II, III, IV y V de esta orden para su

presentación en papel y de sus equivalentes en formato electrónico, así como la aprobación de otros formularios que, en su caso, resulten precisos para la gestión de dicho registro.

Estos formularios serán publicados en el Punto de Acceso General de la Administración General del Estado (https://administracion.gob.es).

Disposición adicional tercera. *Comunicación previa de creación de un Registro Electrónico de Apoderamientos particular.*

Los organismos públicos y entidades de derecho público estatales que a la entrada en vigor de esta orden no cuenten con un Registro Electrónico de Apoderamientos particular y decidan crearlo con posterioridad, deberán comunicarlo a la Dirección General de Gobernanza Pública y a la Secretaría General de Administración Digital con una antelación mínima de un mes a la fecha prevista de entrada en funcionamiento para garantizar su interoperabilidad técnica y que se puedan realizar los ajustes necesarios sin merma del servicio.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas todas las normas de igual o inferior rango en lo que contradigan o se opongan a lo dispuesto en esta orden. En particular, quedan derogadas la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos y la Orden HFP/633/2017, de 28 de junio, por la que se aprueban los modelos de poderes inscribibles en el Registro Electrónico de Apoderamientos de la Administración General del Estado y en el Registro Electrónico de Apoderamientos de las Entidades Locales y se establecen los sistemas de firma válidos para realizar los apoderamientos apud acta a través de medios electrónicos.

Disposición final única. *Entrada en vigor.*

Esta orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Inscripción del Poder[1]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[2] _____; ante funcionario/a con N.R.P[2]:_____

Comparece/n: ☐ Poderdante/s ☐ Apoderado/a

1) Identificación de las personas poderdantes

Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:
Teléfono:	Correo electrónico:	
Domicilio:		

Nota: En el caso de apoderamientos de varias personas físicas (poderdantes) a una persona física o jurídica, incluir los datos identificativos anteriores de cada uno de ellos.

2) La/las persona/s poderdante/s otorga/n poder a favor de la persona apoderada (elija una de las dos opciones)

☐ Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:
Teléfono:	Correo electrónico:	
Domicilio:		

[1] La presentación de este modelo en papel en una Oficina de Asistencia en Materia de Registros sólo será posible en el caso de comparecencia de poderdante o apoderado/a persona física.
[2] A cumplimentar por la Administración.

☐ Persona jurídica:

Identificación de la persona jurídica	
NIF:	
Denominación social:	
Teléfono:	Correo electrónico:

3) Poder

Tan amplio y bastante como en Derecho sea necesario para actuar en nombre de la persona poderdante para la realización de las siguientes actuaciones (señale uno de los tres tipos de poderes):

☐ A) Poder general para que la persona apoderada pueda actuar en nombre del poderdante en cualquier actuación administrativa y ante cualquier Administración Pública.

☐ B) Poder para que la persona apoderada pueda actuar en nombre de la persona poderdante en cualquier actuación administrativa (elija una opción y complete los datos):

☐ Opción 1: Ante la Administración General del Estado y todos los organismos públicos o entidades de derecho público vinculados o dependientes[3].

☐ Opción 2: Ante un Organismo público o Entidad de derecho público vinculado o dependiente concreto[3].

(Denominación del organismo o entidad)	Código DIR3[4]:

[3] Organismos públicos y entidades de derecho público vinculados o dependientes que no cuenten con un Registro Electrónico de Apoderamientos particular. Puede consultar estos organismos a través del Punto de Acceso General de la Administración General del Estado (http://administracion.gob.es) o en el 060.

[4] Los códigos DIR3 serán cumplimentados por la Administración.

☐ C) Poder para que la persona apoderada pueda actuar en nombre de la persona poderdante únicamente para la realización de los siguientes trámites ante un órgano, Organismo público o Entidad de derecho público vinculado o dependiente.

(Denominación del órgano, organismo o entidad)	Código DIR3:
Trámites[5] del órgano, organismo o entidad: (para seleccionar todos los trámites escriba la palabra TODOS[6]) ……	Códigos SIA: ……

4) Vigencia del poder

La vigencia máxima no podrá superar los cinco años a contar desde la fecha de inscripción. La fecha de inicio consignada tendrá valor siempre que sea posterior a la fecha de inscripción.

Fecha de inicio: / /	Fecha fin: / /

5) En caso de aportarse documento público o privado con firma legitimada notarial[7]

Debe hacerse constar los siguientes datos:

Código Seguro de Validación (CSV):

[5] Puede consultar el listado de trámites objeto de apoderamiento a través del Punto de Acceso General de la Administración General del Estado (http://administracion.gob.es) o en el 060.
[6] Se refiere a todos los trámites que pueden ser objeto de apoderamiento.
[7] Sólo se aportarán estos datos en el caso de solicitud presentada por persona apoderada.

En caso de no aportar un CSV, datos del poder notarial:

Nombre:	1.º apellido:	2.º apellido:
Colegio:		
N.º Protocolo:	Fecha de otorgamiento: / /	
Teléfono:	Correo electrónico:	
Dirección:		

☐ Poder notarial: Se adjunta documento notarial debidamente firmado.

6) Firma dela persona apoderada[8]

Con la firma del presente escrito acepta la representación conferida.

En _____, __/_____/_____

7) Firma de la/las persona/s poderdante/s[9]

En _____, __/_____/_____

[8] Cuando la solicitud sea presentada por el/la poderdante, la persona apoderada podrá realizar la aceptación en el mismo momento de presentación o, en otro momento, aportando el modelo del Anexo IV en papel debidamente cumplimentado y firmado; o a través de internet.
[9] En el caso de apoderamientos otorgados mediante documento público o privado con firma legitimada notarial no será necesaria la firma de poderdante o poderdantes.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES

En cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO I

Para la cumplimentación y tramitación de la inscripción, se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada apoderamiento que el/la ciudadano/a (persona física) desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

c) Los datos de teléfono y correo electrónico se utilizarán para contactar con el/la interesado/a. En el caso de personas físicas, estos datos son opcionales.

ANEXO II

Revocación de poder[10]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[11] _____; ante funcionario/a con NRP[11]:_____

1) Comparece la persona poderdante

Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

La persona poderdante REVOCA el poder otorgado en fecha __/__/____, con número: _____, otorgado en favor de la persona apoderada (elija una de las opciones):

☐ Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

☐ Persona jurídica:

Identificación de la persona jurídica
NIF:
Denominación social:

2) Firma de la persona poderdante

En _____, __/_____/_____

[10] La presentación de este modelo en papel ante una Oficina de Asistencia en Materia de Registros sólo será posible en el caso de poderdante persona física.

[11] A cumplimentar por la Administración.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO II

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada revocación que el/la ciudadano/a desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

ANEXO III

Renuncia del poder[12]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[13] _____; ante funcionario/a con NRP[13]:_____.

1) Comparece la persona apoderada

Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

El/la apoderado/a RENUNCIA al poder otorgado en fecha: __/__/____, con número: _____, otorgado a su favor, por la persona poderdante:

☐ Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

2) Firma de la persona apoderada

En _____, __/_____/_____

[12] La presentación de este modelo en papel ante una Oficina de Asistencia en Materia de Registros solo será posible en el caso de apoderado/a persona física que actúe en nombre de otra persona física no obligada a relacionarse electrónicamente.

[13] A cumplimentar por la Administración.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre el Registro Electrónico de Apoderamientos y protección de datos en la sede del Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO III

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada renuncia que el/la ciudadano/a desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

ANEXO IV

Aceptación por la persona apoderada[14]

Presentado en la Oficina de Asistencia en Materia de Registros n.º[15] _____; ante funcionario/a con NRP[15]:_____.

1) Comparece la persona apoderada.

Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

El/la apoderado/a ACEPTA el poder otorgado en fecha: __/__/____, con número: _____, a su favor, por la persona poderdante:

☐ Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

2) Firma de la persona apoderada

Con la firma del presente escrito acepta la representación conferida.

En _____, __/_____/_____

[14] La presentación de este modelo en papel, ante una Oficina de Asistencia en Materia de Registros, sólo será posible en el caso de apoderado/a persona física.
[15] A cumplimentar por la Administración.

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1 e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO IV

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada aceptación que el/la ciudadano/a desee realizar ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

ANEXO V

Prórroga de un Poder[16]

Presentado en la Oficina de Asistencia en Materia de Registros nº[17] _____; ante funcionario/a con N.R.P[17]:_____.

1) Comparece la persona poderdante. Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

El poderdante PRORROGA el poder otorgado en fecha __/__/____, con número: _____, en favor de la persona apoderada (elija una de las opciones):

☐ Persona física mayor de edad:

DNI/NIE:		
Nombre:	1.º apellido:	2.º apellido:

☐ Persona jurídica:

Identificación persona jurídica
NIF:
Denominación social:

La vigencia máxima no podrá superar los cinco años a contar desde la fecha de inscripción.

2) Prórroga del poder hasta[18]: / /

[16] La presentación de este modelo en papel ante una Oficina de Asistencia en Materia de Registros sólo será posible en el caso de poderdante persona física.

[17] A cumplimentar por la Administración.

[18] La vigencia del poder, incluidas las prórrogas, no podrá exceder de 5 años desde la fecha de inscripción.

3) Firma de la persona poderdante

En _____, __/_____/_____

INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS PERSONALES en cumplimiento del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (RGPD).

Finalidad: gestión de solicitudes de inscripción de poderes y la acreditación de la representación en los términos de los artículos 11 y 12 de la orden.

Legitimación: cumplimiento de una obligación legal [art. 6.1.e)] RGPD.

Destinatarios: persona, órgano o unidad administrativa al que se dirigen los documentos registrados.

Derechos: de acceso, rectificación, supresión y el resto de derechos que pueden encontrarse en la siguiente página web: https://administracion.gob.es

Más información sobre protección de datos en el Punto de Acceso General de la Administración General del Estado.

INSTRUCCIONES DE CUMPLIMENTACIÓN DEL ANEXO V

Se atenderán las siguientes instrucciones:

a) Se cumplimentará un ejemplar por cada prórroga que el/la ciudadano/a desee realizar a ante el/la funcionario/a de la Oficina de Asistencia en Materia de Registros, consignando, en cada caso, todos los datos que se requieren en el presente modelo de formulario.

b) El/la funcionario/a de la oficina entregará al/la ciudadano/a un justificante registrado y sellado con la fecha y el número del registro de entrada correspondiente.

§ 23

Orden TES/388/2022, de 29 de abril, por la que se regula el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A

Ministerio de Trabajo y Economía Social
«BOE» núm. 107, de 5 de mayo de 2022
Última modificación: sin modificaciones
Referencia: BOE-A-2022-7318

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, ha establecido una regulación completa y sistemática de las relaciones *ad extra* entre las Administraciones públicas y los administrados, cuya finalidad principal es la simplificación y agilización de los procedimientos administrativos.

A este respecto, la ley prevé que los interesados con capacidad de obrar podrán actuar por medio de representante ante las Administraciones públicas, y la forma de su acreditación mediante el apoderamiento *apud acta,* presencial o electrónico, y su inscripción en el registro electrónico de apoderamientos de la Administración Pública competente.

Asimismo, se establece la información mínima que deben contener los asientos que se realicen en los registros electrónicos de apoderamientos, y la tipología de los poderes que se inscriban, que pueden ser: Poderes generales para que el apoderado pueda realizar en nombre del poderdante cualquier actuación administrativa y ante cualquier Administración; poderes que permiten al apoderado actuar en nombre del poderdante para cualquier actuación administrativa ante una Administración u organismo concreto; y poderes que permiten al apoderado actuar en nombre del poderdante únicamente para la realización de determinados trámites especificados en el poder.

De acuerdo con la ley, los registros electrónicos generales de apoderamientos no impedirán la existencia de registros electrónicos particulares en cada organismo, donde se inscribirán los poderes otorgados para la realización de actuaciones generales o trámites específicos ante el mismo.

Por otra parte, el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, aprobado por el Real Decreto 203/2021, de 30 de marzo, prevé, en su artículo 33.3, que cada organismo público o entidad de derecho público vinculado o dependiente de la Administración General del Estado podrá disponer de un registro particular de apoderamientos en el que se inscriban los poderes otorgados por quien ostente la condición de interesado para realizar los trámites específicos de su competencia y cuya gestión corresponderá al propio organismo o entidad. En estos registros particulares no podrán inscribirse los poderes previstos en el artículo 6.4.a) de la Ley 39/2015, de 1 de octubre.

De acuerdo con el citado reglamento, los registros electrónicos generales y particulares de apoderamientos pertenecientes a todas las Administraciones, deben ser plenamente interoperables entre sí, de modo que se garantice su interconexión, compatibilidad informática, así como la transmisión telemática de las solicitudes, escritos y comunicaciones,

y permitirán comprobar válidamente la representación de quienes actúen ante las Administraciones Públicas en nombre de un tercero.

En consideración a tales previsiones y en el marco del impulso al empleo de los medios electrónicos, informáticos y telemáticos en las relaciones entre el Fondo de Garantía Salarial, O.A. y la ciudadanía, mediante la presente orden se procede a crear el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A.

Esta orden se adecua a los principios de buena regulación previstos en el artículo 129.1 de la Ley 39/2015, de 1 de octubre, al ajustarse a los principios de eficacia y proporcionalidad, en tanto que es el instrumento más adecuado para acometer el objetivo que se persigue, consistente en adecuar el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A. a las disposiciones del Reglamento de actuación y funcionamiento del sector público por medios electrónicos y conforme a la Ley 39/2015, de 1 de octubre.

Asimismo, su regulación se adecúa a los principios de seguridad jurídica y eficiencia, al ser coherente con el resto del ordenamiento jurídico, estar sus objetivos claramente definidos y responder a la finalidad de mejorar el servicio público, al permitir a los interesados formalizar apoderamientos y acreditar representaciones en favor de terceros, no imponiéndoles nuevas cargas administrativas.

Finalmente, la orden se ajusta al principio de transparencia y se ha sometido al trámite de audiencia e información pública, de acuerdo con lo establecido en el artículo 26.6 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

La orden ha sido informada favorablemente por la Comisión Ministerial de Administración Digital, conforme a lo establecido por el artículo 2.2.j) de la Orden TES/1214/2021, de 29 de octubre, por la que se crea la Comisión Ministerial de Administración Digital y se regula su composición y funciones.

También ha sido informada por la Agencia Española de Protección de Datos, de acuerdo con lo previsto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en el artículo 5.3.b) del Estatuto de la indicada Agencia, aprobado por el Real Decreto 389/2021, de 1 de junio.

Asimismo, ha sido informada por la Subdirección General de Tecnologías de la Información y Comunicaciones del Ministerio de Trabajo y Economía Social, dependiente de la Subsecretaría de Trabajo y Economía Social, de acuerdo con lo previsto por el artículo 5.5.e) del Real Decreto 499/2020, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Trabajo y Economía Social, y se modifica el Real Decreto 1052/2015, de 20 de noviembre, por el que se establece la estructura de las Consejerías de Empleo y Seguridad Social en el exterior y se regula su organización, funciones y provisión de puestos de trabajo.

El desarrollo de la aplicación informática para el registro electrónico de apoderamientos del Fondo de Garantía Salarial se enmarca en el Plan de digitalización de la Administración General del Estado 2021-2025, Eje 2-Proyectos de alto impacto en la Digitalización del Sector Público, medida 12 –Transformación digital en Materia de empleo, concretamente en el proyecto APSS Móviles, Inteligencia Artificial y Satisfacción Ciudadana– Mejorar la satisfacción del usuario en el uso de servicios públicos digitales.

El Plan de Digitalización de la Administración General del Estado es uno de los elementos principales del Componente 11, Modernización de las Administraciones Públicas del Plan de Recuperación, Transformación y Resiliencia, quedando incluido el mencionado desarrollo informático en el Proyecto 11, Subproyecto 2, de la Inversión 2, Proyectos tractores de digitalización de la Administración General del Estado, del citado Componente.

La actuación descrita se ha llevado a cabo de conformidad con la regulación contenida en la Orden Ministerial HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia, así como la propia de la Orden HFP/1031/2021, de 29 de septiembre, por la que por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.

Esta orden se dicta en ejercicio de la atribución conferida por la disposición final del Real Decreto 505/1985, de 6 de marzo, sobre organización y funcionamiento del Fondo de Garantía Salarial, que faculta a la Ministra de Trabajo y Economía Social para dictar las disposiciones necesarias para el desarrollo de dicho real decreto.

En su virtud, con la aprobación previa de la Ministra de Hacienda y Función Pública, dispongo:

Artículo 1. *Objeto y ámbito de aplicación.*

1. Esta orden tiene por objeto regular los requisitos y condiciones de funcionamiento del Registro Electrónico de apoderamientos del Fondo de Garantía Salarial, O.A. (en adelante, el Registro), en el que se inscribirán los apoderamientos que de forma voluntaria se otorguen apud acta a favor de un tercero, presencial o electrónicamente, por quien ostente la condición de interesado en un procedimiento administrativo para actuar en su nombre ante el Fondo de Garantía Salarial, O.A.

2. El Registro será único en el ámbito del Fondo de Garantía Salarial, O.A., y será accesible en la sede electrónica del organismo (en adelante sede electrónica). El Registro no tiene carácter público, por lo que solo la persona interesada, una vez identificada, podrá consultarlo electrónica o presencialmente, y acceder a la información de los apoderamientos de los que sea poderdante o apoderada.

3. Las representaciones legales no serán objeto de inscripción en el Registro.

Artículo 2. *Tipos de apoderamientos a inscribir en el registro.*

En el registro podrán inscribirse los siguientes tipos de apoderamientos:

a) Apoderamiento general, para que el apoderado pueda llevar a cabo en nombre del poderdante cualquier actuación administrativa en todas las materias, trámites y grupos de trámites recogidos en el anexo I relacionados con el Fondo de Garantía Salarial, O.A., sin que se pueda renunciar o revocar el poder por separado respecto a alguno de ellos.

b) Apoderamiento por materias, para que el apoderado pueda actuar en nombre del poderdante y llevar a cabo cualquiera de los trámites y/o grupos de trámites en la materia seleccionada de entre las relacionadas en el anexo I, sin que se pueda renunciar o revocar el poder por separado respecto a alguno de estos trámites.

c) Apoderamiento por trámites y/o grupos de trámites, para que el apoderado pueda actuar en nombre del poderdante solo en aquellos trámites y/o grupos de trámites seleccionados de entre los relacionados en el anexo I, pudiéndose renunciar o revocar el poder por separado respecto a cualquiera de ellos.

Artículo 3. *Órganos competentes.*

1. Corresponde a la Secretaría General del Fondo de Garantía Salarial, O.A., la titularidad y gestión del Registro, así como la aprobación y modificación de los modelos que resulten precisos para su adecuada gestión.

2. La Unidad de Informática de la Secretaría General garantizará la disponibilidad y accesibilidad del Registro; la identificación de los interesados mediante métodos de identificación admitidos en la sede electrónica; la integridad de los datos incorporados; la generación de evidencias electrónicas que permitan la constatación de la fecha y hora de los accesos y actuaciones relevantes para la incorporación de tales datos, así como la generación de documentos electrónicos que acrediten los poderes inscritos en el Registro.

Artículo 4. *Poderdantes y apoderados.*

1. Podrán otorgar apoderamiento las personas físicas, jurídicas y entidades sin personalidad jurídica que ostenten capacidad de obrar y que tengan la condición de interesados en relación con las materias, trámites y/o grupos de trámites relacionados en el anexo I.

2. Podrán ser apoderados las personas físicas que ostenten capacidad de obrar, así como las personas jurídicas cuando, además, tengan prevista en sus estatutos la posibilidad de actuar en representación de un tercero ante las Administraciones públicas.

Artículo 5. *Apoderamientos. Otorgamiento y otras actuaciones.*

1. A efectos de su inscripción en el registro, los apoderamientos que se otorguen apud acta podrán efectuarse de las siguientes formas:

a) Mediante comparecencia electrónica en la sede electrónica a través del uso de los métodos de identificación y firma admitidos en ella.

Si el compareciente fuese una persona jurídica o una entidad sin personalidad jurídica, la identificación y firma se realizarán mediante el uso de certificados cualificados de representante, como medio de acreditar la representación y capacidad para realizar las actuaciones en el registro.

b) Mediante comparecencia de la persona física en las oficinas de asistencia en materia de registros del Fondo de Garantía Salarial, O.A., donde el compareciente, una vez identificado por el funcionario habilitado, firmará la correspondiente solicitud. En este caso, el funcionario habilitado será responsable de la inscripción.

c) Mediante comparecencia de la persona física en las oficinas de asistencia en materia de registros de otras Administraciones públicas u organismos, para la posterior remisión del poder al Registro, a efectos de su inscripción, siendo el funcionario habilitado a tal fin responsable de esta.

La modificación de los datos y de la vigencia de los apoderamientos otorgados, así como la consulta sobre sus términos y situación y las demás actuaciones relativas a los mismos reguladas en esta orden, tales como su aceptación, renuncia y revocación, podrán llevarse a cabo en las formas señaladas en el apartado anterior.

Artículo 6. *Inscripción de los apoderamientos.*

1. El poderdante podrá solicitar la inscripción en el Registro del apoderamiento otorgado en las formas previstas en el artículo 5.

2. Desde el Registro se comunicará al apoderado el otorgamiento del poder a su favor, advirtiéndole, cuando proceda, de la necesidad de presentar la declaración responsable a que se refiere el apartado 5 de este artículo y de aceptar expresamente el apoderamiento en los supuestos a que se refiere el artículo 11.

A efectos de la comunicación indicada en el párrafo anterior, el poderdante deberá facilitar los datos de contacto del apoderado.

3. Los poderes surtirán efectos ante el Fondo de Garantía Salarial, O.A. desde la fecha de su inscripción en el Registro y respecto de las materias, trámites y/o grupos de trámites a los que expresamente se refieran y que hayan sido seleccionados de entre los relacionados en el anexo I y publicados en la sede electrónica.

4. El apoderado, cuando sea una persona obligada a relacionarse electrónicamente con la Administración, deberá solicitar electrónicamente la inscripción en el Registro del apoderamiento. Cuando el apoderamiento derive de un documento público notarial o de una certificación expedida por un registro mercantil, el interesado deberá aportar la certificación registral electrónica correspondiente o el código seguro u otro sistema de acceso y verificación del documento electrónico.

5. Los poderes otorgados en favor de profesionales, personas físicas o jurídicas, no se inscribirán ni surtirán efecto hasta que el poderdante proceda a presentar una declaración responsable manifestando de forma inequívoca que acepta ser representado por el apoderado ante el Fondo de Garantía Salarial, O.A., detallando las facultades delegadas.

6. Los apoderamientos que requieran aceptación expresa por parte del apoderado no se inscribirán ni surtirán efecto hasta que se produzca dicha aceptación, en los términos señalados en el artículo 11.

Artículo 7. *Requisitos de la declaración responsable.*

La declaración responsable deberá firmarse electrónicamente o bien mediante comparecencia física en la Unidad Administrativa Periférica correspondiente del Fondo de Garantía Salarial, O.A., en la que el compareciente, una vez identificado por el funcionario habilitado, firmará la declaración con carácter previo a la presentación de la solicitud de prestaciones de garantía salarial o de otros ámbitos sectoriales competencia del Organismo.

En caso de presentarse nuevas solicitudes de registro de apoderamientos a favor de la misma persona física o jurídica, no será necesaria la presentación de una nueva declaración responsable, siempre y cuando se mantengan los requisitos de capacidad que la sustentan. La declaración responsable podrá realizarse utilizando el anexo VI de esta orden.

La declaración responsable sustituirá a la presentación de los poderes, sin perjuicio de que éstos puedan ser exigidos con posterioridad por el órgano competente del Fondo de Garantía Salarial, O.A. En este caso, deberá constar en el Registro el resultado de la comprobación realizada.

Artículo 8. *Representaciones otorgadas.*

Con el fin de que el Fondo de Garantía Salarial, O.A., pueda verificar la validez de las representaciones otorgadas, y toda vez que éstas deriven de un documento público notarial o de una certificación expedida por un registro mercantil, el interesado deberá aportar la certificación registral electrónica correspondiente o expresar el código seguro u otro sistema de acceso y verificación del documento electrónico.

El Fondo de Garantía Salarial, O.A., efectuará la verificación de la autenticidad e integridad del traslado a papel y el acceso a los metadatos necesarios para la tramitación automatizada de la certificación registral electrónica, mediante el acceso electrónico y gratuito a la dirección electrónica que el Consejo General del Notariado o el Colegio de Registradores, respectivamente, habrán de tener habilitada a tales efectos.

Asimismo, cuando necesite comprobar la vigencia, revocación o cese de representaciones inscritas en el Registro Mercantil, consultará electrónicamente y de modo gratuito el Registro Mercantil.

Artículo 9. *Contenido del registro.*

1. El Registro estará disponible en la sede electrónica, donde se mantendrá una relación pública y actualizada de todas las materias, trámites y/o grupos de trámites de la competencia del Fondo de Garantía Salarial, O.A., que pueden ser objeto de apoderamiento.

2. En los asientos que se realicen para inscribir un apoderamiento en el Registro se harán constar los siguientes datos:

a) Nombre y apellidos, denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del poderdante, así como sus datos de contacto.

b) Nombre y apellidos, denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del apoderado, así como sus datos de contacto.

c) Materias, trámites y/o grupos de trámites objeto de apoderamiento.

d) Periodo de vigencia del poder.

e) Número de referencia del poder asignado por el Registro.

f) Fecha de inscripción en el Registro.

g) Estado del poder.

h) Tipo de poder según las facultades que otorgue.

Artículo 10. *Plazo de vigencia de los apoderamientos inscritos en el registro.*

1. Los poderes inscritos en el Registro tendrán una vigencia máxima de cinco años, a contar desde la fecha de su inscripción.

2. En cualquier momento antes de la finalización del plazo señalado en el apartado anterior el poderdante podrá modificar, revocar o prorrogar la vigencia del apoderamiento, en cuyo caso podrá solicitar la modificación de su plazo de vigencia en las formas previstas en el artículo 5.

3. Las prórrogas otorgadas por el poderdante tendrán una validez determinada, sin que esta pueda ser superior a cinco años contados desde la fecha de inscripción de la prórroga en el Registro.

Artículo 11. *Aceptación expresa del apoderamiento.*

1. La aceptación expresa del apoderado resultará necesaria en los supuestos en los que el apoderamiento comprenda la recepción de comunicaciones o notificaciones, sea cual sea la naturaleza del procedimiento.

2. El apoderado deberá aceptar expresamente el apoderamiento en el plazo máximo de un mes desde su otorgamiento, en las formas previstas en el artículo 5.

En estos casos, el apoderamiento solo se inscribirá y surtirá efectos desde la fecha en que conste esa aceptación en el Registro.

Artículo 12. *Renuncia y revocación del apoderamiento.*

La renuncia por el apoderado a un apoderamiento inscrito en el Registro y la revocación de este por el poderdante efectuadas en las formas previstas en el artículo 5, solo surtirán efectos desde la fecha en que se produzca la inscripción de la renuncia o la revocación en el Registro. La renuncia y la revocación podrán realizarse utilizando el formulario consignado en el anexo IV de esta orden.

Artículo 13. *Consulta al registro por parte de los interesados y obtención de certificados de poderes registrados.*

Los interesados podrán consultar de forma electrónica los datos relativos a la inscripción, contenido y vigencia del poder o poderes inscritos en los que figuren como poderdantes o apoderados, así como obtener certificados de los apoderamientos inscritos en el Registro.

Artículo 14. *Protección de datos de carácter personal.*

1. De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos (Reglamento general de protección de datos), y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando la persona poderdante o la apoderada tuvieran condición de personas físicas, la licitud del tratamiento se fundamenta en el artículo 6.1.e) del Reglamento. El tratamiento de datos personales que resulte necesario para el adecuado funcionamiento del Registro y su finalidad está fundado en el cumplimiento de una misión realizada en interés público y en el ejercicio de poderes públicos conferidos al responsable derivados de una competencia atribuida por una norma con rango de ley.

Los datos personales recogidos en el Registro no podrán tratarse para una finalidad diferente a la acreditación de la existencia y vigencia de un apoderamiento inscrito, debiendo suprimirse, sin dilación, en los supuestos de revocación, renuncia o finalización del plazo de vigencia del apoderamiento.

2. Previo análisis de los riesgos para los derechos y libertades de las personas físicas, se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Las medidas a implantar como consecuencia del análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad, deberán prevalecer sobre estas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de protección de datos.

3. La Secretaría General del Fondo de Garantía Salarial, O.A. es la responsable del tratamiento, siendo la Unidad de Informática de la Secretaría General la encargada del tratamiento.

4. El anexo VII contiene el encargo de tratamiento, de acuerdo con lo dispuesto en el artículo 28 del Reglamento general de protección de datos.

Artículo 15. *Aprobación de modelos.*

1. Se aprueban los siguientes modelos inscribibles en el registro, en función de los distintos tipos de apoderamientos a que se refiere el artículo 2 y de las actuaciones a realizar respecto a ellos:

a) Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante el Fondo de Garantía Salarial, O.A. de cualquier trámite en todas o en algunas de las materias relacionadas en el anexo I, y que figura como anexo II.

b) Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante el Fondo de Garantía Salarial, O.A. de determinados trámites, de entre los relacionados en el anexo I, y que figura como anexo III.

c) Aceptación, renuncia y revocación de poderes otorgados, que figura como anexo IV.

d) Modificación del plazo de vigencia de poderes otorgados, que figura como anexo V.

2. Asimismo, a efecto de lo establecido en el artículo 6.5, se aprueba un modelo de declaración responsable susceptible de cumplimentación potestativa por el poderdante, que figura como anexo VI.

3. Cuando la comparecencia personal tenga lugar en las oficinas de asistencia en materia de registros de otra Administración pública u organismo a que se refiere el artículo 5.1.c), los modelos presentados en dicho registro serán enviados mediante intercambio registral al Fondo de Garantía Salarial, O.A., a efectos de su posterior inclusión en el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A.

Artículo 16. *Cancelación de las inscripciones.*

En los supuestos de fallecimiento, alteración o extinción de capacidad de obrar del poderdante o apoderado por cualquiera de las causas previstas en Derecho, así como en los casos de desaparición de la personalidad jurídica de la sociedad, se iniciará el procedimiento de cancelación de las inscripciones de apoderamiento.

A este efecto, el Fondo de Garantía Salarial, O.A., podrá verificar de forma gratuita y mediante consulta al Registro Civil Central la posible concurrencia de circunstancias modificativas o impeditivas de dicha capacidad.

Disposición adicional única. *Incremento gasto público.*

Esta orden implica incremento de gasto público y su ejecución se llevará a cabo con cargo al concepto presupuestario 692 correspondiente al capítulo 6 del Presupuesto de Gastos del Fondo de Garantía Salarial, O.A., para el ejercicio 2022. No supone disminución de ingreso alguno para la Hacienda Pública Estatal y se llevará a cabo con las disponibilidades presupuestarias existentes.

Disposición final primera. *Facultades de aplicación.*

Se faculta a la persona titular de la Secretaría General del Fondo de Garantía Salarial, O.A., para dictar cuantas resoluciones resulten necesarias para la aplicación y ejecución de lo previsto en esta orden y para actualizar sus anexos.

Disposición final segunda. *Entrada en vigor.*

La presente orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Relación de trámites susceptibles de apoderamiento

Materia	Trámites
Prestaciones de garantía salarial.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba. Recibir notificaciones y comunicaciones.
Contratación.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba, recibir notificaciones y comunicaciones relativas a los procedimientos relacionados con la contratación pública realizada por el Fondo de Garantía Salarial, O.A.
Patrimonio.	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba, recibir notificaciones y comunicaciones relativos a los negocios patrimoniales con el Fondo de Garantía Salarial, O.A.
Reclamaciones y recursos.	Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones respecto a actos dictados por el Fondo de Garantía Salarial, O.A.

Materia	Descripción
Prestaciones de garantía salarial	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento del derecho a las prestaciones del Fondo de Garantía Salarial, O.A., así como para su revisión. Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos de revisión de prestaciones del Fondo de Garantía Salarial, O.A. y de reclamación de prestaciones indebidas.
Contratación.	El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por el Fondo de Garantía Salarial, O.A.
Patrimonio	El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con el Fondo de Garantía Salarial, O.A.
Reclamaciones y recursos.	El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por el Fondo de Garantía Salarial, O.A.

Trámite	Descripción
Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	El apoderado puede presentar, subsanar o completar solicitudes, escritos, declaraciones y comunicaciones, acompañando, en su caso, los documentos acreditativos requeridos o que considere oportunos. También puede desistir de las solicitudes presentadas. Igualmente puede aportar a un procedimiento administrativo datos, documentos y elementos de prueba, formular alegaciones y, en su caso, participar en el trámite de audiencia. Asimismo, puede realizar cualquier otro trámite o actuación administrativa prevista en la legislación aplicable, incluido el abono de una obligación o el cobro de una cantidad líquida.
Recibir notificaciones y comunicaciones.	El apoderado puede recibir las notificaciones de resolución o actos administrativos que ponen fin a los procedimientos o que implican efectos jurídicos y cuya fecha de recepción por parte del interesado marca el inicio del plazo para poder presentar reclamaciones o recursos. Asimismo, puede recibir todas aquellas comunicaciones informativas, sin efectos jurídicos, que la entidad que gestiona el procedimiento pueda remitir al interesado. El apoderamiento de este trámite implica que las notificaciones y/o comunicaciones se realizarán por vía electrónica al apoderado, conforme a la regulación específica de dicha materia.
Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones.	El apoderado puede presentar escritos de reclamación y recursos contra resoluciones y actos de trámite en los casos legalmente previstos, intervenir en todos sus trámites, formular alegaciones y desistir de los mismos, así como recibir las notificaciones y comunicaciones que puedan generarse respecto a los recursos y reclamaciones formulados.

ANEXO II

Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante el Fondo de Garantía Salarial, O.A., de cualquier trámite en todas o algunas de las materias que se especifican

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar (**todos los datos son obligatorios):**

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Teléfono: *	Correo electrónico: *
Domicilio:		
Código Postal:	Localidad:	Provincia:

*Es opcional y su falta de cumplimentación no impide la inscripción del poder

☐ Persona jurídica o entidad sin personalidad jurídica que ostente capacidad de obrar (**todos los datos son obligatorios):**

Identificación de la persona jurídica:		
Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		
Identificación de la persona jurídica:		
NIF:	Razón Social:	
Teléfono:	Correo electrónico:	

****

El poderdante otorga poder a favor de (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar (**todos los datos son obligatorios):**

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Correo electrónico:	

☐ Persona jurídica que ostente capacidad de obrar (**todos los datos son obligatorios):**

NIF:	Razón Social:
Correo electrónico:	

Poder
Tan amplio y bastante como en Derecho sea necesario para actuar en nombre del poderdante para la realización de cualquier trámite en las materias seleccionadas a continuación

Elija una de las dos opciones siguientes:

□ Materia general que abarca todas las gestiones con el Fondo de Garantía Salarial, O.A.
□ Materia(s) concreta(s) incluidas en el ámbito del Fondo de Garantía Salarial, O.A. (elija una o varias opciones):

	Materia	Descripción
□	**Prestaciones de garantía salarial**	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento del derecho a las prestaciones del Fondo de Garantía Salarial, O.A., así como para su revisión. Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos de revisión de prestaciones del Fondo de Garantía Salarial, O.A. y de reclamación de prestaciones indebidas.
□	**Contratación.**	El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por el Fondo de Garantía Salarial, O.A.
□	**Patrimonio**	El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con el Fondo de Garantía Salarial, O.A.
□	**Reclamaciones y recursos.**	El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por el Fondo de Garantía Salarial, O.A.

Vigencia del Poder

Fecha de fin **A rellenar por el poderdante** **XX/XX/XXXX**	La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A.

Firma del poderdante:

En _____, ____/____/____

Lugar Fecha

ANEXO III

Poder para que el apoderado pueda actuar en nombre del poderdante para la realización ante el Fondo de Garantía Salarial, O.A., de determinados trámites

Comparece el poderdante (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar (**todos los datos son obligatorios):**

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Teléfono: *	Correo electrónico: *
Domicilio:		
Código Postal:	Localidad:	Provincia:

*Es opcional y su falta de cumplimentación no impide la inscripción del poder

☐ Persona jurídica o entidad sin personalidad jurídica que ostente capacidad de obrar (**todos los datos son obligatorios):**

Identificación de la persona jurídica:		
Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:		
Identificación de la persona jurídica:		
NIF:	Razón Social:	
Teléfono:	Correo electrónico:	

****

El poderdante otorga poder a favor de (elija una de las dos opciones):

☐ Persona física que ostente capacidad de obrar (**todos los datos son obligatorios):**

Nombre:	Primer apellido:	Segundo apellido:
DNI/NIF/Documento equivalente:	Correo electrónico:	

☐ Persona jurídica que ostente capacidad de obrar (**todos los datos son obligatorios):**

NIF:	Razón Social:
Correo electrónico:	

Poder

Tan amplio y bastante como en Derecho sea necesario para actuar en nombre del poderdante para la realización de los trámites seleccionados a continuación (elija una o varias opciones)

Materia*	Trámites*	
Prestaciones de garantía salarial	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	☐
	Recibir notificaciones y comunicaciones.	☐
Contratación	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba relativas a los procedimientos relacionados con la contratación pública realizada por el Fondo de Garantía Salarial, O.A.	☐
	Recibir notificaciones y comunicaciones relativas a los procedimientos relacionados con la contratación pública realizada por el Fondo de Garantía Salarial, O.A.	☐
Patrimonio	Presentar solicitudes, realizar alegaciones o aportar elementos de prueba relativos a los negocios patrimoniales con el Fondo de Garantía Salarial, O.A.	☐
	Recibir notificaciones y comunicaciones relativos a los negocios patrimoniales con el Fondo de Garantía Salarial, O.A.	☐
Reclamaciones y recursos	Presentar reclamaciones y recursos, realizar alegaciones o aportar elementos de prueba respecto a actos dictados por el Fondo de Garantía Salarial, O.A.	☐
	Recibir notificaciones y comunicaciones respecto a actos dictados por el Fondo de Garantía Salarial, O.A.	☐

*NOTA: Consulte la descripción de materias y trámites al final de este formulario

Vigencia del Poder

Fecha de fin **A rellenar por el poderdante** **XX/XX/XXXX**	La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A.

Firma del poderdante:

En _____, ____/____/____

Lugar Fecha

Materia	Descripción
Todas las gestiones con el Fondo de Garantía Salarial, O.A.	El apoderado podrá realizar todas las actuaciones en cualquier materia y trámite ante el Fondo de Garantía Salarial, O.A.
Prestaciones de garantía salarial.	El apoderado podrá realizar actuaciones, intervenir en procedimientos o efectuar trámites para el reconocimiento del derecho a las prestaciones del Fondo de Garantía Salarial, O.A., así como para su revisión. Asimismo, podrá realizar todas esas actuaciones en relación con los procedimientos de revisión de prestaciones del Fondo de Garantía Salarial, O.A. y de reclamación de prestaciones indebidas.
Contratación.	El apoderado podrá realizar actuaciones relativas a los procedimientos relacionados con la contratación pública realizada por el Fondo de Garantía Salarial, O.A.
Patrimonio.	El apoderado podrá realizar actuaciones y efectuar trámites relativos a los negocios patrimoniales con el Fondo de Garantía Salarial, O.A.
Reclamaciones y recursos.	El apoderado podrá realizar todos los trámites (presentación, alegaciones, prueba, desistimiento, etc.) y recibir las notificaciones y comunicaciones administrativas relativas a los recursos y reclamaciones formulados frente a actos dictados por el Fondo de Garantía Salarial, O.A.

Trámites	Descripción
Presentar solicitudes, realizar alegaciones o aportar elementos de prueba.	El apoderado puede presentar, subsanar o completar solicitudes, escritos, declaraciones y comunicaciones, acompañando, en su caso, los documentos acreditativos requeridos o que considere oportunos. También puede desistir de las solicitudes presentadas. Igualmente puede aportar a un procedimiento administrativo datos, documentos y elementos de prueba, formular alegaciones y, en su caso, participar en el trámite de audiencia. Asimismo, puede realizar cualquier otro trámite o actuación administrativa prevista en la legislación aplicable, incluido el abono de una obligación o el cobro de una cantidad líquida.
Recibir notificaciones y comunicaciones.	El apoderado puede recibir las notificaciones de resolución o actos administrativos que ponen fin a los procedimientos o que implican efectos jurídicos y cuya fecha de recepción por parte del interesado marca el inicio del plazo para poder presentar reclamaciones o recursos. Asimismo, puede recibir todas aquellas comunicaciones informativas, sin efectos jurídicos, que el Fondo de Garantía Salarial, O.A. pueda remitir al interesado. El apoderamiento de este trámite implica que las notificaciones y/o comunicaciones se realizarán por vía electrónica al apoderado, conforme a la regulación específica de dicha materia.
Presentar reclamaciones y recursos, realizar alegaciones y recibir notificaciones o comunicaciones.	El apoderado puede presentar escritos de reclamación y recursos contra resoluciones y actos de trámite en los casos legalmente previstos, intervenir en todos sus trámites, formular alegaciones y desistir de los mismos, así como recibir las notificaciones y comunicaciones que puedan generarse respecto a los recursos y reclamaciones formulados.

ANEXO IV

Aceptación, renuncia y revocación del poder otorgado

Elija solo una de las siguientes operaciones:

Poderdante

☐ Revocación de poder(es)

Apoderado

☐ Aceptación de poder(es)

☐ Renuncia de poder(es).

****

Identificación del compareciente

☐ Persona física que ostente capacidad de obrar (todos los datos son obligatorios):

Nombre:	Primer Apellido:	Segundo Apellido:
DNI/NIF/Documento equivalente		

☐ Persona jurídica o entidad sin personalidad jurídica -como poderdante- que ostente capacidad de obrar (todos los datos son obligatorios):

Identificación del representante		
Nombre:	Primer Apellido:	Segundo Apellido:
DNI/NIF/Documento equivalente		
Identificación de la persona jurídica		
CIF	Razón Social	

Indique a continuación los poderes afectados por la operación seleccionada separados por comas.

Numero de referencia de los poderes

Efectos de la operación desde la fecha de inscripción en el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A.

Firma del poderdante:

En _____, ____/____/____

Lugar Fecha

ANEXO V

Modificación de plazo de poderes otorgados

Comparece el poderdante (elija una de las dos opciones):

□ Persona física que ostente capacidad de obrar **(todos los datos son obligatorios):**

Nombre:	Primer Apellido:	Segundo Apellido:
DNI/NIF/Documento equivalente		

□ Persona jurídica o entidad sin personalidad jurídica -como poderdante- que ostente capacidad de obrar (**todos los datos son obligatorios):**

Identificación del representante		
Nombre:	Primer Apellido:	Segundo Apellido:
DNI/NIF/Documento equivalente		
Identificación de la persona jurídica		
CIF	Razón Social	

****

Indique a continuación los poderes afectados (una línea para cada poder).

La vigencia máxima no podrá superar los cinco años a contar desde la fecha de la inscripción en el Registro electrónico de apoderamientos de la Seguridad Social.

Número de referencia de los poderes:	**Fecha de fin de los poderes (días/mes/año)**
	/ /
	/ /
	/ /
	/ /

Efectos de la operación desde la fecha de inscripción en el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, O.A.

Firma del poderdante:

En _____, ____/____/____

Lugar Fecha

ANEXO VI

Modelo de declaración responsable recogido en el artículo 6.5 de la Orden ministerial por la que se regula el Registro electrónico de apoderamientos del Fondo de Garantía Salarial, en el que el poderdante acepta ser representado por el apoderado ante el Fondo de Garantía Salarial, O.A., para todos/algunos de los trámites y actuaciones recogidos en su anexo I

D/D.ª _____, con DNI _____, actuando en nombre propio o como representante de (para las personas jurídicas) _____ con (CIF:_____).

Datos de contacto:

–Domicilio: _____

– Teléfono:*_____

– Correo electrónico:* _____

Forma en que desea recibir las notificaciones:

☐ Por correo postal ☐ Electrónicamente (las personas obligadas a relacionarse electrónicamente con la Administración en virtud del artículo 14 de la Ley 39/2015, de 1 de octubre, recibirán las notificaciones electrónicamente independientemente de la forma que elijan).

Declara responsablemente:

Que Don/Doña _____ con DNI/NIE _____ ostenta los requisitos de capacidad jurídica y de obrar para actuar como mi representante en los trámites y actuaciones ante el Fondo de Garantía Salarial, O.A., designados en el anexo I, II o III.

Datos del poder o documento notarial: certificación registral electrónica correspondiente, código seguro u otro sistema de acceso y verificación del documento electrónico: _____

_____

Para que conste, a los efectos de dar cumplimiento al artículo 6.5 de la referida orden ministerial:

En _____, ____/____/____

Lugar Fecha Firma del poderdante:

**es opcional y su falta de cumplimentación no impide la inscripción del poder*

ANEXO VII

Protección de datos de carácter personal

A) Tratamiento de datos. De conformidad con lo dispuesto en los artículos 13 y 14 del Reglamento General de Protección de Datos, y 22.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales le informamos que:

– El órgano responsable del tratamiento de sus datos personales es la Secretaría General del Fondo de Garantía Salarial, O.A.

– La finalidad del tratamiento es la seguridad y conservación de los datos personales existentes en el Registro Electrónico de Apoderamientos del Fondo de Garantía Salarial, O.A., y la utilización de los mismos limitada a las inscripciones y revocaciones de los apoderamientos.

– La base jurídica del tratamiento es la contenida en el artículo 6.1.e) del Reglamento General de Protección de Datos: el cumplimiento de una misión de interés público.

– El destinatario de sus datos de carácter personal es la Secretaría General del Fondo de Garantía Salarial, O.A.

– No están previstas las transferencias internacionales de datos.

– El plazo de conservación de sus datos será de un mes, transcurrido el cual serán eliminados.

– Las medidas de seguridad implantadas están a su disposición en el Área de Informática de la Secretaría General del Fondo de Garantía Salarial, O.A.

– Puede ejercer su derecho de acceso, rectificación o supresión, o la limitación de su tratamiento, o a oponerse al mismo. Le recordamos su derecho a presentar una reclamación ante la Agencia Española de Protección de Datos.

B) Cláusulas.

1. Objeto. El presente anexo tiene por objeto definir, de conformidad con lo dispuesto en el artículo 28 del RGPD y el resto de normativa de protección de datos que resulte aplicable, las condiciones conforme a las cuales el encargado del tratamiento, bajo las instrucciones del responsable del tratamiento, llevará a cabo el tratamiento de datos personales que resulten necesarios para la prestación del objeto del contrato.

2. Obligaciones del encargado del tratamiento. El encargado de tratamiento, llevará a cabo el tratamiento de datos personales, de conformidad con las siguientes obligaciones:

– Se compromete a tratar los datos personales siguiendo instrucciones documentadas del responsable, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.

– Se compromete a garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad.

– Se compromete a tomar todas las medidas necesarias de conformidad con el artículo 32 del Reglamento Europeo de Protección de Datos; en concreto, las relativas a la implementación de todas aquellas actuaciones necesarias para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: la seudonimización y el cifrado de datos personales, la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico, un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

– Se compromete a acatar las limitaciones establecidas en los numerales 2 y 4 del artículo 32 para el caso de que el encargado del tratamiento recurra a otro encargado.

– Se compromete a asistir al responsable teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que éste pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

– Se compromete a ayudar al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del Reglamento Europeo de Protección de Datos, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

– Se compromete, a elección del responsable, a suprimir o devolver todos los datos personales una vez concluya la prestación de los servicios de tratamiento y a suprimir las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

– Se compromete a poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

§ 24

Orden PRE/878/2010, de 5 de abril, por la que se establece el régimen del sistema de dirección electrónica habilitada previsto en el artículo 38.2 del Real Decreto 1671/2009, de 6 de noviembre

Ministerio de la Presidencia
«BOE» núm. 88, de 12 de abril de 2010
Última modificación: sin modificaciones
Referencia: BOE-A-2010-5788

Una de las manifestaciones más relevantes de la Administración electrónica es la práctica de notificaciones por medios electrónicos, informáticos y telemáticos por las distintas Administraciones Públicas. Esta posibilidad, vislumbrada en el artículo 70 de la Ley 30/1992, cobró carta de naturaleza específica cuando la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, incorporo sendos textos de idéntico tenor en los artículos 105 de la Ley General Tributaria y 59 de la Ley 30/1992, configurando un nuevo modelo de notificación mediante la puesta a disposición de la actuación correspondiente de manera que los efectos de la notificación se producen bien por el acceso a su contenido bien por el simple transcurso del lapso de diez días desde la puesta a disposición sin que tenga lugar dicho acceso por parte del destinatario. El Real Decreto 209/2003, de 21 de febrero, desarrolla esta última previsión, siendo su disposición final primera desarrollada a su vez por la Orden PRE/1551/2003, de 10 de junio, con el objeto de establecer los requisitos de autenticidad, integridad, disponibilidad y confidencialidad de los dispositivos y aplicaciones de registro y notificación, así como los protocolos y criterios técnicos a los que deben sujetarse y las condiciones que han de reunir el órgano, organismo o entidad habilitada para la prestación del servicio de dirección electrónica única así como las condiciones de su prestación. Toda la regulación de la notificación electrónica se fundamenta en la existencia de una única dirección electrónica a tal efecto en el ámbito de la Administración del Estado y en su carácter voluntario.

La Ley 11/2007, de 11 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, regula de modo similar la notificación por medios electrónicos, admitiendo que en determinados supuestos pueda establecerse esta notificación con carácter obligatorio. El reciente Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, desarrolla en su artículo 38 la notificación mediante la puesta a disposición del documento electrónico a través de dirección electrónica habilitada, previendo que bajo responsabilidad del Ministerio de la Presidencia existirá un sistema de dirección electrónica habilitada para la práctica de estas notificaciones que quedará a disposición de todos los órganos y organismos públicos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios. Además, en su apartado segundo se establece que «Cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, la dirección electrónica habilitada a que se refiere el apartado anterior será asignada de oficio y podrá tener vigencia indefinida, conforme al régimen que

se establezca por la orden del Ministro de la Presidencia a la que se refiere la disposición final primera».

En su virtud, previo informe del Consejo Superior de Administración Electrónica, dispongo:

Artículo 1. *Objeto.*

La presente Orden tiene por objeto establecer el régimen de un sistema de notificación mediante dirección electrónica habilitada, a disposición de los órganos y organismos vinculados o dependientes de la Administración General del Estado que no establezcan sistemas de notificación propios, tanto en los casos de notificación voluntaria como cuando tenga carácter obligatorio, de acuerdo con lo previsto en el artículo 38 y en la disposición final primera del Real Decreto 1671/2009, de 8 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Artículo 2. *Dirección electrónica habilitada responsabilidad del Ministerio de la Presidencia.*

1. La titularidad de la dirección electrónica a partir de la cual se construyan las direcciones electrónicas habilitadas de los interesados, corresponde al Ministerio de la Presidencia.

2. La prestación del servicio de dirección electrónica habilitada se llevará a cabo por el Ministerio de la Presidencia, directamente, o a través del prestador que se establezca conforme a lo dispuesto en el ordenamiento jurídico.

3. El directorio del servicio de dirección electrónica habilitada deberá recoger el nombre y apellidos o la razón o denominación social del interesado, el número de identificación fiscal y la dirección electrónica habilitada.

4. El sistema de dirección electrónica habilitada se sujetará a lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como a la normativa protectora en materia de datos de carácter personal.

Artículo 3. *Asignación de dirección electrónica habilitada.*

1. Se asignará una dirección electrónica habilitada, con la inclusión en el correspondiente directorio, cuando el interesado solicite su apertura.

2. Asimismo se asignará en todo caso de oficio una dirección electrónica cuando se reciba de un órgano u organismo de la Administración General del Estado el aviso para la práctica de una notificación conforme al sistema establecido en la presente Orden.

Artículo 4. *Vigencia.*

1. La dirección electrónica habilitada tendrá vigencia indefinida, excepto en los supuestos en que se solicite su revocación por el titular, por fallecimiento de la persona física o extinción de la personalidad jurídica, que una resolución administrativa o judicial así lo ordene o por el transcurso de tres años sin que se utilice para la práctica de notificaciones, supuesto en el cual se inhabilitará esta dirección electrónica, comunicándose así al interesado.

2. No obstante, no se inhabilitará esta dirección electrónica cuando se establezca la práctica de notificaciones electrónicas con carácter obligatorio, y así se confirme por los órganos u organismos afectados al prestador del servicio de dirección electrónica.

Artículo 5. *Autenticación.*

1. La identificación y autenticación de la notificación se hará por alguno de los medios admitidos conforme a la ley 11/2007 y de acuerdo con lo establecido por el Real Decreto 1671/2009.

2. La autenticación de los ciudadanos en el acceso al contenido del documento notificado se hará mediante certificados electrónicos que se admitan conforme a lo establecido en la normativa vigente.

3. En particular, las personas jurídicas y entidades sin personalidad podrán acceder al contenido del documento notificado mediante los certificados electrónicos que se admitan.

Artículo 6. *Confidencialidad.*

1. El sistema de notificación electrónica contendrá mecanismos de cifrado para proteger la confidencialidad de los datos en las transmisiones.

2. Asimismo, el sistema contará con las medidas de seguridad adecuadas para que el prestador del servicio de dirección electrónica habilitada no acceda al contenido de los actos y actuaciones administrativas que se notifiquen.

Artículo 7. *Referencia temporal.*

1. El sistema de notificación electrónica acreditará las fechas y horas en que se produzca la puesta a disposición del interesado del acto objeto de notificación. Ello tendrá lugar mediante la recepción en la dirección electrónica asignada al destinatario del aviso de la puesta a disposición de la notificación, incluyendo el propio documento que se notifica o, al menos, su huella electrónica.

Para la referencia temporal de los actos y certificaciones se utilizará una marca de tiempo entendiendo por tal la asignación por medios electrónicos de la fecha y, en su caso, la hora. La fecha y hora utilizada se sincronizará con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio del Real Instituto y Observatorio de la Armada como laboratorio depositario del patrón Nacional de Tiempo y laboratorio asociado al Centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

La información relativa a las marcas de tiempo se asociará en la forma que determine el Esquema Nacional de Interoperabilidad.

2. El sistema de dirección electrónica habilitada acreditará igualmente el acceso del destinatario al contenido del documento notificado, así como cualquier causa técnica que imposibilite alguna de las circunstancias de este artículo.

Artículo 8. *Seguridad.*

1. Los órganos de la Administración General del Estado y los organismos públicos vinculados o dependientes de aquélla que pongan en marcha dispositivos y aplicaciones de registro y notificación deben adoptar medidas de seguridad para la salvaguarda de la confidencialidad. En cualquier caso establecerán las siguientes medidas:

a) Medidas de seguridad física.

b) Control de los accesos a los dispositivos y aplicaciones de registro y notificación, en especial los que lleguen a través de las redes de comunicaciones.

c) Protección de los soportes de información y copias de respaldo.

d) Cifrado de las notificaciones, cuando así se establezca por la legislación sobre protección de los datos de carácter personal o lo estime necesario el órgano u organismo notificador.

2. El prestador del servicio de dirección electrónica única designará a un responsable de la seguridad, que se encargará de la realización y actualización del análisis y gestión de riesgos, del registro de incidencias de seguridad, de la correcta implementación de las salvaguardas de seguridad técnicas, organizativas, y de cuantas otras actuaciones en materia de seguridad sean necesarias para la protección de los sistemas a su cargo.

Artículo 9. *Disponibilidad.*

1. El sistema de dirección electrónica habilitada posibilitará el acceso permanente de los interesados a la dirección electrónica correspondiente, tanto para solicitar la asignación de una dirección electrónica habilitada como para acceder al contenido de las notificaciones puestas a su disposición.

2. El acceso se producirá a través del Punto de Acceso General de la Administración General del Estado, así como de las sedes electrónicas del Ministerio de la Presidencia y de

los órganos u organismos adheridos al sistema o, en su caso, del prestador del servicio de dirección electrónica.

3. Los órganos y organismos a los que se refiere el artículo anterior adoptarán las medidas organizativas y técnicas para garantizar la disponibilidad del servicio 7 días a la semana y 24 horas al día, y en cualquier caso las siguientes:

a) Adopción de medidas de protección frente a código dañino en los servidores de aplicación y en los soportes circulantes.

b) Preparación y mantenimiento operativo de un plan de contingencia.

Artículo 10. *Condiciones de prestación del servicio.*

1. El órgano, organismo o entidad al que, en su caso, corresponda la prestación del sistema de dirección electrónica habilitada, llevará a cabo las siguientes funciones:

a) Crear y mantener el directorio de direcciones electrónica habilitadas con la información proporcionada por los interesados.

b) Almacenar y custodiar los avisos de puesta a disposición en la dirección electrónica habilitada.

c) Gestionar los acuses de recibo de los interesados y de los órganos u organismos notificadores.

d) Mantener el registro de eventos de las notificaciones, el cual contendrá, al menos, la dirección electrónica, la traza de la fecha y la hora de la recepción de la puesta a disposición en la dirección electrónica y del acceso del interesado a la notificación y la descripción del contenido de la notificación.

e) Impedir el acceso al contenido de las notificaciones que se entienden rechazadas por el transcurso de diez días desde su puesta a disposición.

f) Establecer las medidas organizativas y técnicas para que la disponibilidad del servicio sea de siete días a la semana y veinticuatro horas al día.

g) Potestativamente, otras funciones de mejora del servicio y complementarias de las expresadas, como es el caso de aviso de puesta a disposición de los interesados de las notificaciones mediante mensajería o de cualquier otro modo.

2. El prestador del servicio de dirección electrónica habilitada deberá remitir al órgano u organismo actuante por cada notificación electrónica:

a) Certificación electrónica de la fecha y hora en la que recibe el aviso de puesta a disposición enviada por el órgano u organismo notificador.

b) Certificación electrónica de la fecha y hora en la que se produce la recepción en la dirección electrónica asignada al destinatario del aviso de la puesta a disposición de la notificación, incluyendo el propio acto o actuación notificada o, al menos, su sello electrónico.

c) Certificación electrónica en la que conste la fecha y hora en la que se produce el acceso del interesado al contenido de la notificación en la dirección electrónica.

d) Certificación electrónica del transcurso del plazo de diez días desde la puesta a disposición sin que se haya producido el acceso del interesado al contenido de la notificación en la dirección electrónica.

e) Certificación electrónica de cualquier incidencia que se produzca en la práctica de lo dispuesto en los apartados anteriores.

3. En el caso de cese de actividad o cambio del prestador del servicio de dirección electrónica, las bases de datos, los programas informáticos asociados, el registro de eventos y el dominio de direcciones electrónicas con las notificaciones que existan en ese momento y la documentación técnica, deberán entregarse al Ministerio de la Presidencia, o a la entidad que éste designe debidamente actualizadas.

4. Los programas necesarios para el correcto funcionamiento del sistema de notificación serán suministrados a los órganos y organismos notificadores por el prestador del servicio de dirección electrónica habilitada.

Disposición transitoria única. *Mantenimiento de la prestación del servicio.*

1. A la entrada en vigor de la presente Orden, la prestación del servicio de dirección habilitada seguirá realizándose a través de los servicios autorizados, de conformidad con la Orden PRE/1551/2003, de 10 de junio, por la que se desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, por la que se regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.

2. En el plazo de tres meses desde la entrada en vigor de la presente Orden se llevarán a cabo las adaptaciones requeridas en la prestación del servicio de dirección habilitada.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en esta Orden, y, especialmente, la Orden PRE/1551/2003, de 10 de junio, que desarrolla la disposición final primera del Real Decreto 209/2003, de 21 de febrero, que regula los registros y notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de certificados por los ciudadanos.

Disposición final. *Entrada en vigor.*

La presente orden entrará en vigor al día siguiente al de su publicación en el «Boletín Oficial del Estado».

Madrid, 5 de abril de 2010.–La Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, María Teresa Fernández de la Vega Sanz.

§ 25

Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español

Jefatura del Estado
«BOE» núm. 155, de 29 de junio de 1985
Última modificación: 12 de octubre de 2021
Referencia: BOE-A-1985-12534

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren,

Sabed: Que las Cortes generales han aprobado y Yo vengo en sancionar la siguiente Ley:

PREÁMBULO

El Patrimonio Histórico Español es el principal testigo de la contribución histórica de los españoles a la civilización universal y de su capacidad creativa contemporánea. La protección y el enriquecimiento de los bienes que lo integran constituyen obligaciones fundamentales que vinculan a todos los poderes públicos, según el mandato que a los mismo dirige el artículo 46 de la norma constitucional.

Exigencias, que en el primer tercio del siglo constituyeron para el legislador un mandato similar, fueron ejemplarmente cumplidas por los protagonistas de nuestra mejor tradición intelectual, jurídica y democrática, como es buena muestra el positivo legado recibido de la Ley de 13 de mayo de 1933. Pese a este reconocimiento, lo cierto es que la recuperación por nuestro pueblo de su libertad determinó que, desde los primeros momentos en que tan feliz proceso histórico se consumó, se emprendiera la tarea de elaborar una nueva y más amplia respuesta legal a tales exigencias, un verdadero código de nuestro Patrimonio Histórico, en el que los proyectos de futuro se conformaran a partir de las experiencias acumuladas.

Su necesidad fue sentida, en primer término, a causa de la dispersión normativa que, a lo largo del medio siglo transcurrido desde la entrada en vigor de la venerable Ley, ha producido en nuestro ordenamiento jurídico multitud de fórmulas con que quisieron afrontarse situaciones concretas en aquel momento no previstas o inexistentes. Deriva asimismo esta obligación de la creciente preocupación sobre esta materia por parte de la comunidad internacional y de sus organismos representativos, la cual ha generado nuevos criterios para la protección y enriquecimiento de los bienes históricos y culturales, que se han traducido en Convenciones y Recomendaciones, que España ha suscrito y observa, pero a las que su legislación interna no se adaptaba. La revisión legal queda, por último, impuesta por una nueva distribución de competencias entre Estado y Comunidades Autónomas que,

en relación a tales bienes, emana de la Constitución y de los Estatutos de Autonomía. La presente Ley es dictada, en consecuencia, en virtud de normas contenidas en los apartados 1 y 2 del artículo 149 de nuestra Constitución, que para el legislador y la Administración estatal suponen tanto un mandato como un título competencial.

Esta Ley consagra una nueva definición de Patrimonio Histórico y amplía notablemente su extensión. En ella quedan comprendidos los bienes muebles e inmuebles que los constituyen, el Patrimonio Arqueológico y el Etnográfico, los Museos, Archivos y Bibliotecas de titularidad estatal, así como el Patrimonio Documental y Bibliográfico. Busca, en suma, asegurar la protección y fomentar la cultura material debida a la acción del hombre en sentido amplio, y concibe aquélla como un conjunto de bienes que en sí mismos han de ser apreciados, sin establecer limitaciones derivadas de su propiedad, uso, antigüedad o valor económico.

Ello no supone que las medidas de protección y fomento se desplieguen de modo uniforme sobre la totalidad de los bienes que se consideran integrantes, en virtud de la Ley, de nuestro Patrimonio Histórico. La Ley establece distintos niveles de protección que se corresponden con diferentes categorías legales. La más genérica y que da nombre a la propia Ley es la de Patrimonio histórico Español, constituido éste por todos aquellos bienes de valor histórico, artístico, científico o técnico que conforman la aportación de España a la cultura universal. En torno a ese concepto se estructuran las medidas esenciales de la Ley y se precisan las técnicas de intervención que son competencia de la Administración del Estado, en particular, su defensa contra la exportación ilícita y su protección frente a la expoliación.

En el seno del Patrimonio Histórico Español, y al objeto de otorgar una mayor protección y tutela, adquiere un valor singular la categoría de Bienes de Interés Cultural, que se extiende a los muebles e inmuebles de aquel Patrimonio que, de forma más palmaria, requieran tal protección. Semejante categoría implica medidas asimismo singulares que la Ley establece según la naturaleza de los bienes sobre los cuales recae.

La Ley dispone también las fórmulas necesarias para que esa valoración sea posible, pues la defensa del Patrimonio Histórico de un pueblo no debe realizarse exclusivamente a través de normas que prohíban determinadas acciones o limiten ciertos usos, sino a partir de disposiciones que estimulen a su conservación y, en consecuencia, permitan su disfrute y faciliten su acrecentamiento.

Así, la Ley estipula un conjunto de medidas tributarias y fiscales y abre determinados cauces nuevos que colocan a España en un horizonte similar al que ahora se contempla en países próximos al nuestro por su historia y su cultura y, en consecuencia, por su acervo patrimonial. De esa forma se impulsa una política adecuada para gestionar con eficacia el Patrimonio Histórico Español. Una política que complemente la acción vigilante con el estímulo educativo, técnico y financiero, en el convencimiento de que el Patrimonio Histórico se acrecienta y se defiende mejor cuanto más lo estiman las personas que conviven con él, pero también cuantas más ayudas se establezcan para atenderlo, con las lógicas contraprestaciones hacia la sociedad cuando son los poderes públicos quienes facilitan aquéllas.

El Patrimonio Histórico Español es una riqueza colectiva que contiene las expresiones más dignas de aprecio en la aportación histórica de los españoles a la cultura universal. Su valor lo proporciona la estima que, como elemento de identidad cultural, merece a la sensibilidad de los ciudadanos, porque los bienes que lo integran se han convertido en patrimoniales debido exclusivamente a la acción social que cumplen, directamente derivada del aprecio con que los mismos ciudadanos los han ido revalorizando.

En consecuencia, y como objetivo último, la Ley no busca sino el acceso a los bienes que constituyen nuestro Patrimonio Histórico. Todas las medidas de protección y fomento que la Ley establece sólo cobran sentido si, al final, conducen a que un número cada vez mayor de ciudadanos pueda contemplar y disfrutar las obras que son herencia de la capacidad colectiva de un pueblo. Porque en un Estado democrático estos bienes deben estar adecuadamente puestos al servicio de la colectividad en el convencimiento de que con su disfrute se facilita el acceso a la cultura y que ésta, en definitiva, es camino seguro hacia la libertad de los pueblos.

TITULO PRELIMINAR

Disposiciones Generales

Artículo primero.

1. Son objeto de la presente Ley la protección, acrecentamiento y transmisión a las generaciones futuras del Patrimonio Histórico Español.

2. Integran el Patrimonio Histórico Español los inmuebles y objetos muebles de interés artístico, histórico, paleontológico, arqueológico, etnográfico, científico o técnico. También forman parte del mismo el patrimonio documental y bibliográfico, los yacimientos y zonas arqueológicas, así como los sitios naturales, jardines y parques, que tengan valor artístico, histórico o antropológico.

Asimismo, forman parte del Patrimonio Histórico Español los bienes que integren el Patrimonio Cultural Inmaterial, de conformidad con lo que establezca su legislación especial.

3. Los bienes más relevantes del Patrimonio Histórico Español deberán ser inventariados o declarados de interés cultural en los términos previstos en esta Ley.

Artículo segundo.

1. Sin perjuicio de las competencias que correspondan a los demás poderes públicos, son deberes y atribuciones esenciales de la Administración del Estado, de conformidad con lo establecido en los artículos 46 y 44, 149.1.1, y 149.2 de la Constitución, garantizar la conservación del Patrimonio Histórico Español, así como promover el enriquecimiento del mismo y fomentar y tutelar el acceso de todos los ciudadanos a los bienes comprendidos en él. Asimismo, de acuerdo con lo dispuesto en el artículo 149.1, 28, de la Constitución, la Administración del Estado protegerá dichos bienes frente a la exportación ilícita y la expoliación.

2. En relación al Patrimonio Histórico Español, la Administración del Estado adoptará las medidas necesarias para facilitar su colaboración con los restantes poderes públicos y la de éstos entre sí, así como para recabar y proporcionar cuanta información fuera precisa a los fines señalados en el párrafo anterior.

3. A la Administración del Estado compete igualmente la difusión internacional del conocimiento de los bienes integrantes del Patrimonio Histórico Español, la recuperación de tales bienes cuando hubiesen sido ilícitamente exportados y el intercambio, respecto a los mismos, de información cultural, técnica y científica con los demás Estados y con los Organismos internacionales, de conformidad con lo establecido en el artículo 149.1, número 3, de la Constitución. Las demás Administraciones competentes colaborarán a estos efectos con la Administración del Estado.

Artículo tercero.

1. La comunicación y el intercambio de programas de actuación e información relativos al Patrimonio Histórico Español serán facilitados por el Consejo del Patrimonio Histórico, constituido por un representante de cada Comunidad Autónoma, designado por su Consejo de Gobierno, y el Director General correspondiente de la Administración del Estado, que actuará como Presidente.

2. Sin perjuicio de las funciones atribuidas al Consejo del Patrimonio Histórico, son instituciones consultivas de la Administración del Estado, a los efectos previstos en la presente Ley, la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español, las Reales Academias, las Universidades españolas, el Consejo Superior de Investigaciones Científicas y las Juntas Superiores que la Administración del Estado determine por vía reglamentaria, y en lo que pueda afectar a una Comunidad Autónoma, las instituciones por ella reconocidas. Todo ello con independencia del asesoramiento que, en su caso, pueda recabarse de otros organismos profesionales y entidades culturales.

Artículo cuarto.

A los efectos de la presente Ley se entiende por expoliación toda acción u omisión que ponga en peligro de pérdida o destrucción todos o alguno de los valores de los bienes que

integran el Patrimonio Histórico Español, o perturbe el cumplimiento de su función social. En tales casos la Administración del Estado, con independencia de las competencias que correspondan a las Comunidades Autónomas, en cualquier momento, podrá interesar del Departamento competente del Consejo de Gobierno de la Comunidad Autónoma correspondiente la adopción con urgencia de las medidas conducentes a evitar la expoliación. Si se desatendiere el requerimiento, la Administración del Estado dispondrá lo necesario para la recuperación y protección, tanto legal como técnica, del bien expoliado.

Artículo quinto.

1. A los efectos de la presente Ley se entiende por exportación la salida del territorio español de cualquiera de los bienes que integran el Patrimonio Histórico Español.

2. Los propietarios o poseedores de tales bienes con más de cien años de antigüedad y, en todo caso, de los inscritos en el Inventario General previsto en el artículo 26 de esta Ley precisarán para su exportación autorización expresa y previa de la Administración del Estado en la forma y condiciones que se establezcan por vía reglamentaria.

3. No obstante lo dispuesto en el apartado anterior, y sin perjuicio de lo que establecen los artículos 31 y 34 de esta Ley, queda prohibida la exportación de los bienes declarados de interés cultural, así como la de aquellos otros que, por su pertenencia al Patrimonio Histórico Español, la Administración del Estado declare expresamente inexportables, como medida cautelar hasta que se incoe expediente para incluir el bien en alguna de las categorías de protección especial previstas en esta Ley.

Artículo sexto.

A los efectos de la presente Ley se entenderá como Organismos competentes para su ejecución:

a) Los que en cada Comunidad Autónoma tengan a su cargo la protección del patrimonio histórico.

b) Los de la Administración del Estado, cuando así se indique de modo expreso o resulte necesaria su intervención para la defensa frente a la exportación ilícita y la expoliación de los bienes que integran el Patrimonio Histórico Español. Estos Organismos serán también los competentes respecto de los bienes integrantes del Patrimonio Histórico Español adscritos a servicios públicos gestionados por la Administración del Estado o que formen parte del Patrimonio Nacional.

Artículo séptimo.

Los Ayuntamientos cooperarán con los Organismos competentes para la ejecución de esta Ley en la conservación y custodia del Patrimonio Histórico Español comprendido en su término municipal, adoptando las medidas oportunas para evitar su deterioro, pérdida o destrucción. Notificarán a la Administración competente cualquier amenaza, daño o perturbación de su función social que tales bienes sufran, así como las dificultades y necesidades que tengan para el cuidado de estos bienes. Ejercerán asimismo las demás funciones que tengan expresamente atribuidas en virtud de esta Ley.

Artículo octavo.

1. Las personas que observen peligro de destrucción o deterioro en un bien integrante del Patrimonio Histórico Español deberán, en el menor tiempo posible, ponerlo en conocimiento de la Administración competente, quien comprobará el objeto de la denuncia y actuará con arreglo a lo que en esta Ley se dispone.

2. Será pública la acción para exigir ante los órganos administrativos y los Tribunales Contencioso-Administrativos el cumplimiento de lo previsto en esta Ley para la defensa de lo bienes integrantes del Patrimonio Histórico Español.

TITULO I

De la declaración de Bienes de Interés Cultural

Artículo noveno.

1. Gozarán de singular protección y tutela los bienes integrantes del Patrimonio Histórico Español declarados de interés cultural por ministerio de esta Ley o mediante Real Decreto de forma individualizada.

2. La declaración mediante Real Decreto requerirá la previa incoación y tramitación de expediente administrativo por el Organismo competente, según lo dispuesto en el artículo 6.º de esta Ley. En el expediente deberá constar informe favorable de alguna de las Instituciones consultivas señaladas en el artículo 3.º, párrafo 2.º, vr o que tengan reconocido idéntico carácter en el ámbito de una Comunidad Autónoma. Transcurridos tres meses desde la solicitud del informe sin que éste hubiera sido emitido, se entenderá que el dictamen requerido es favorable a la declaración de interés cultural. Cuando el expediente se refiera a bienes inmuebles se dispondrá, además, la apertura de un período de información pública y se dará audiencia al Ayuntamiento interesado.

3. El expediente deberá resolverse en el plazo máximo de veinte meses a partir de la fecha en que hubiere sido incoado. La caducidad del expediente se producirá transcurrido dicho plazo si se ha denunciado la mora y siempre que no haya recaído resolución en los cuatro meses siguientes a la denuncia. Caducado el expediente no podrá volver a iniciarse en los tres años siguientes, salvo a instancia del titular.

4. No podrá ser declarada Bien de Interés Cultural la obra de un autor vivo, salvo si existe autorización expresa de su propietario o media su adquisición por la Administración.

5. De oficio o a instancia del titular de un interés legítimo y directo, podrá tramitarse por el Organismo competente expediente administrativo, que deberá contener el informe favorable y razonado de alguna de las instituciones consultivas, a fin de que se acuerde mediante Real Decreto que la declaración de un determinado Bien de Interés Cultural quede sin efecto.

Artículo diez.

Cualquier persona podrá solicitar la incoación de expediente para la declaración de un Bien de Interés Cultural. El Organismo competente decidirá si procede la incoación. Esta decisión y, en su caso, las incidencias y resolución del expediente deberán notificarse a quienes lo instaron.

Artículo once.

1. La incoación de expediente para la declaración de un Bien de Interés Cultural determinará, en relación al bien afectado, la aplicación provisional del mismo régimen de protección previsto para los bienes declarados de interés cultural.

2. La resolución del expediente que declare un Bien de Interés Cultural deberá describirlo claramente. En el supuesto de inmuebles, delimitará el entorno afectado por la declaración y, en su caso, se definirán y enumerarán las partes integrantes, las pertenencias y los accesorios comprendidos en la declaración.

Artículo doce.

1. Los bienes declarados de interés cultural serán inscritos en un Registro General dependiente de la Administración del Estado cuya organización y funcionamiento se determinarán por vía reglamentaria. A este Registro se notificará la incoación de dichos expedientes, que causarán la correspondiente anotación preventiva hasta que recaiga resolución definitiva.

2. En el caso de bienes inmuebles la inscripción se hará por alguno de los conceptos mencionados en el artículo 14.2.

3. Cuando se trate de Monumentos y Jardines Históricos la Administración competente además instará de oficio la inscripción gratuita de la declaración en el Registro de la Propiedad.

Artículo trece.

1. A los bienes declarados de interés cultural se les expedirá por el Registro General un Título oficial que les identifique y en el que se reflejarán todos los actos jurídicos o artísticos que sobre ellos se realicen. Las transmisiones o traslados de dichos bienes se inscribirán en el Registro. Reglamentariamente se establecerá la forma y caracteres de este Título.

2. Asimismo, los propietarios y, en su caso, los titulares de derechos reales sobre tales bienes, o quienes los posean por cualquier título, están obligados a permitir y facilitar su inspección por parte de los Organismos competentes, su estudio a los investigadores, previa solicitud razonada de éstos, y su visita pública, en las condiciones de gratuidad que se determinen reglamentariamente, al menos cuatro días al mes, en días y horas previamente señalados. El cumplimiento de esta última obligación podrá ser dispensado total o parcialmente por la Administración competente cuando medie causa justificada. En el caso de bienes muebles se podrá igualmente acordar como obligación sustitutoria el depósito del bien en un lugar que reúna las adecuadas condiciones de seguridad y exhibición durante un período máximo de cinco meses cada dos años.

TITULO II

De los bienes inmuebles

Artículo catorce.

1. Para los efectos de esta Ley tienen la consideración de bienes inmuebles, además de los enumerados en el artículo 334 del Código Civil, cuantos elementos puedan considerarse consustanciales con los edificios y formen parte de los mismos o de su entorno, o lo hayan formado, aunque en el caso de poder ser separados constituyan un todo perfecto de fácil aplicación a otras construcciones o a usos distintos del suyo original, cualquiera que sea la materia de que estén formados y aunque su separación no perjudique visiblemente al mérito histórico o artístico del inmueble al que están adheridos.

2. Los bienes inmuebles integrados en el Patrimonio Histórico Español pueden ser declarados Monumentos, Jardines, Conjuntos y Sitios Históricos, así como Zonas Arqueológicas, todos ellos como Bienes de Interés Cultural.

Artículo quince.

1. Son Monumentos aquellos bienes inmuebles que constituyen realizaciones arquitectónicas o de ingeniería, u obras de escultura colosal siempre que tengan interés histórico, artístico, científico o social.

2. Jardín Histórico es el espacio delimitado, producto de la ordenación por el hombre de elementos naturales, a veces complementado con estructuras de fábrica, y estimado de interés en función de su origen o pasado histórico o de sus valores estéticos, sensoriales o botánicos.

3. Conjunto Histórico es la agrupación de bienes inmuebles que forman una unidad de asentamiento, continua o dispersa, condicionada por una estructura física representativa de la evolución de una comunidad humana por ser testimonio de su cultura o constituir un valor de uso y disfrute para la colectividad. Asimismo es Conjunto Histórico cualquier núcleo individualizado de inmuebles comprendidos en una unidad superior de población que reúna esas mismas características y pueda ser claramente delimitado.

4. Sitio Histórico es el lugar o paraje natural vinculado a acontecimientos o recuerdos del pasado, a tradiciones populares, creaciones culturales o de la naturaleza y a obras del hombre, que posean valor histórico, etnológico, paleontológico o antropológico.

5. Zona Arqueológica es el lugar o paraje natural donde existen bienes muebles o inmuebles susceptibles de ser estudiados con metodología arqueológica, hayan sido o no extraídos y tanto si se encuentran en la superficie, en el subsuelo o bajo las aguas territoriales españolas.

Artículo dieciséis.

1. La incoación de expediente de declaración de interés cultural respecto de un bien inmueble determinará la suspensión de las correspondientes licencias municipales de parcelación, edificación o demolición en las zonas afectadas, así como de los efectos de las ya otorgadas. Las obras que por razón de fuerza mayor hubieran de realizarse con carácter inaplazable en tales zonas precisarán, en todo caso, autorización de los Organismos competentes para la ejecución de esta Ley.

2. La suspensión a que hace referencia el apartado anterior dependerá de la resolución o caducidad del expediente incoado.

Artículo diecisiete.

En la tramitación del expediente de declaración como Bien de Interés Cultural de un Conjunto Histórico deberán considerarse sus relaciones con el área territorial a que pertenece, así como la protección de los accidentes geográficos y parajes naturales que conforman su entorno.

Artículo dieciocho.

Un inmueble declarado Bien de Interés Cultural es inseparable de su entorno. No se podrá proceder a su desplazamiento o remoción, salvo que resulte imprescindible por causa de fuerza mayor o de interés social y, en todo caso, conforme al procedimiento previsto en el artículo 9.º, párrafo 2.º, de esta Ley.

Artículo diecinueve.

1. En los Monumentos declarados Bienes de Interés Cultural no podrá realizarse obra interior o exterior que afecte directamente al inmueble o a cualquiera de sus partes integrantes o pertenencias sin autorización expresa de los Organismos competentes para la ejecución de esta Ley. Será preceptiva la misma autorización para colocar en fachadas o en cubiertas cualquier clase de rótulo, señal o símbolo, así como para realizar obras en el entorno afectado por la declaración.

2. Las obras que afecten a los Jardines Históricos declarados de interés cultural y a su entorno, así como la colocación en ellos de cualquier clase de rótulo, señal o símbolo, necesitarán autorización expresa de los Organismos competentes para la ejecución de esta Ley.

3. Queda prohibida la colocación de publicidad comercial y de cualquier clase de cables, antenas y conducciones aparentes en los Jardines Históricos y en las fachadas y cubiertas de los Monumentos declarados de interés cultural. Se prohíbe también toda construcción que altere el carácter de los inmuebles a que hace referencia este artículo o perturbe su contemplación.

Artículo veinte.

1. La declaración de un Conjunto Histórico, Sitio Histórico o Zona Arqueológica, como Bienes de Interés Cultural, determinará la obligación para el Municipio o Municipios en que se encontraren de redactar un Plan Especial de Protección del área afectada por la declaración u otro instrumento de planeamiento de los previstos en la legislación urbanística que cumpla en todo caso las exigencias en esta Ley establecidas. La aprobación de dicho Plan requerirá el informe favorable de la Administración competente para la protección de los bienes culturales afectados. Se entenderá emitido informe favorable transcurridos tres meses desde la presentación del Plan. La obligatoriedad de dicho Plan no podrá excusarse en la preexistencia de otro planeamiento contradictorio con la protección, ni en la inexistencia previa del planeamiento general.

2. El Plan a que se refiere el apartado anterior establecerá para todos los usos públicos el orden prioritario de su instalación en los edificios y espacios que sean aptos para ello. Igualmente contemplará las posibles áreas de rehabilitación integrada que permitan la recuperación del área residencial y de las actividades económicas adecuadas. También

deberá contener los criterios relativos a la conservación de fachadas y cubiertas e instalaciones sobre las mismas.

3. Hasta la aprobación definitiva de dicho Plan el otorgamiento de licencias o la ejecución de las otorgadas antes de incoarse el expediente declarativo del Conjunto Histórico, Sitio Histórico o Zona Arqueológica, precisará resolución favorable de la Administración competente para la protección de los bienes afectados y, en todo caso, no se permitirán alineaciones nuevas, alteraciones en la edificabilidad, parcelaciones ni agregaciones.

4. Desde la aprobación definitiva del Plan a que se refiere este artículo, los Ayuntamientos interesados serán competentes para autorizar directamente las obras que desarrollen el planeamiento aprobado y que afecten únicamente a inmuebles que no sean Monumentos ni Jardines Históricos ni estén comprendidos en su entorno, debiendo dar cuenta a la Administración competente para la ejecución de esta Ley de las autorizaciones o licencias concedidas en el plazo máximo de diez días desde su otorgamiento. Las obras que se realicen al amparo de licencias contrarias al Plan aprobado serán ilegales y la Administración competente podrá ordenar su reconstrucción o demolición con cargo al Organismo que hubiera otorgado la licencia en cuestión, sin perjuicio de lo dispuesto en la legislación urbanística sobre las responsabilidades por infracciones.

Artículo veintiuno.

1. En los instrumentos de planeamiento relativos a Conjuntos Históricos se realizará la catalogación, según lo dispuesto en la legislación urbanística, de los elementos unitarios que conforman el Conjunto, tanto inmuebles edificados como espacios libres exteriores o interiores, u otras estructuras significativas, así como de los componentes naturales que lo acompañan, definiendo los tipos de intervención posible. A los elementos singulares se les dispensará una protección integral. Para el resto de los elementos se fijará, en cada caso, un nivel adecuado de protección.

2. Excepcionalmente, el Plan de protección de un Conjunto Histórico podrá permitir remodelaciones urbanas, pero sólo en caso de que impliquen una mejora de sus relaciones con el entorno territorial o urbano o eviten los usos degradantes para el propio Conjunto.

3. La conservación de los Conjuntos Históricos declarados Bienes de Interés Cultural comporta el mantenimiento de la estructura urbana y arquitectónica, así como de las características generales de su ambiente. Se considerarán excepcionales las sustituciones de inmuebles, aunque sean parciales, y sólo podrán realizarse en la medida en que contribuyan a la conservación general del carácter del Conjunto. En todo caso, se mantendrán las alineaciones urbanas existentes.

Artículo veintidós.

1. Cualquier obra o remoción de terreno que se proyecte realizar en un Sitio Histórico o en una Zona Arqueológica declarados Bien de Interés Cultural deberá ser autorizada por la Administración competente para la protección de dichos bienes, que podrá, antes de otorgar la autorización, ordenar la realización de prospecciones y, en su caso, excavaciones arqueológicas, de acuerdo con lo dispuesto en el Título V de la presente Ley.

2. Queda prohibida la colocación de cualquier clase de publicidad comercial, así como de cables, antenas y conducciones aparentes en las Zonas Arqueológicas.

Artículo veintitrés.

1. No podrán otorgarse licencias para la realización de obras que, conforme a lo previsto en la presente Ley, requieran cualquier autorización administrativa hasta que ésta haya sido concedida.

2. Las obras realizadas sin cumplir lo establecido en el apartado anterior serán ilegales y los Ayuntamientos o, en su caso, la Administración competente en materia de protección del Patrimonio Histórico Español podrán ordenar su reconstrucción o demolición con cargo al responsable de la infracción en los términos previstos por la legislación urbanística.

Artículo veinticuatro.

1. Si a pesar de lo dispuesto en el artículo 36 llegara a incoarse expediente de ruina de algún inmueble afectado por expediente de declaración de Bien de Interés Cultural, la Administración competente para la ejecución de esta Ley estará legitimada para intervenir como interesado en dicho expediente, debiéndole ser notificada la apertura y las resoluciones que en el mismo se adopten.

2. En ningún caso podrá procederse a la demolición de un inmueble, sin previa firmeza de la declaración de ruina y autorización de la Administración competente, que no la concederá sin informe favorable de al menos dos de las instituciones consultivas a las que se refiere el artículo 3.

3. Si existiera urgencia y peligro inminente, la entidad que hubiera incoado expediente de ruina deberá ordenar las medidas necesarias para evitar daños a las personas. Las obras que por razón de fuerza mayor hubieran de realizarse no darán lugar a actos de demolición que no sean estrictamente necesarios para la conservación del inmueble y requerirán en todo caso la autorización prevista en el artículo 16.1, debiéndose prever además en su caso la reposición de los elementos retirados.

Artículo veinticinco.

El Organismo competente podrá ordenar la suspensión de las obras de demolición total o parcial o de cambio de uso de los inmuebles integrantes del Patrimonio Histórico Español no declarados de interés cultural. Dicha suspensión podrá durar un máximo de seis meses, dentro de los cuales la Administración competente en materia de urbanismo deberá resolver sobre la procedencia de la aprobación inicial de un plan especial o de otras medidas de protección de las previstas en la legislación urbanística. Esta resolución, que deberá ser comunicada al Organismo que hubiera ordenado la suspensión, no impedirá el ejercicio de la potestad prevista en el artículo 37.2.

TITULO III

De los bienes muebles

Artículo veintiséis.

1. La Administración del Estado, en colaboración con las demás Administraciones competentes, confeccionará el Inventario General de aquellos bienes muebles del Patrimonio Histórico Español no declarados de interés cultural que tengan singular relevancia.

2. A los efectos previstos en el párrafo anterior, las Administraciones competentes podrán recabar de los titulares de derechos sobre los bienes muebles integrantes del Patrimonio Histórico Español el examen de los mismos, así como las informaciones pertinentes, para su inclusión, si procede, en dicho Inventario.

3. Los propietarios y demás titulares de derechos reales sobre bienes muebles de notable valor histórico, artístico, arqueológico, científico, técnico o cultural, podrán presentar solicitud debidamente documentada ante la Administración competente, a fin de que se inicie el procedimiento para la inclusión de dichos bienes en el Inventario General. La resolución sobre esta solicitud deberá recaer en un plazo de cuatro meses.

4. Los propietarios o poseedores de los bienes muebles que reúnan el valor y características que se señalen reglamentariamente quedan obligados a comunicar a la Administración competente la existencia de estos objetos, antes de proceder a su venta o transmisión a terceros. Igual obligación se establece para las personas o entidades que ejerzan habitualmente el comercio de los bienes muebles integrantes del Patrimonio Histórico Español, que deberán, además, formalizar ante dicha Administración un libro de registro de las transmisiones que realicen sobre aquellos objetos.

5. La organización y el funcionamiento del Inventario General se determinarán por vía reglamentaria.

6. A los bienes muebles integrantes del Patrimonio Histórico Español incluidos en el Inventario General se les aplicarán las siguientes normas:

a) La Administración competente podrá en todo momento inspeccionar su conservación.

b) Sus propietarios y, en su caso, los demás titulares de derechos reales sobre los mismos están obligados a permitir su estudio a los investigadores, previa solicitud razonada, y a prestarlos, con las debidas garantías, a exposiciones temporales que se organicen por los Organismos a que se refiere el artículo 6.º de esta Ley. No será obligatorio realizar estos préstamos por un período superior a un mes por año.

c) La transmisión por actos ínter vivos o mortis causa, así como cualquier otra modificación en la situación de los bienes deberá comunicarse a la Administración competente y anotarse en el Inventario General.

Artículo veintisiete.

Los bienes muebles integrantes del Patrimonio Histórico Español podrán ser declarados de interés cultural. Tendrán tal consideración, en todo caso, los bienes muebles contenidos en un inmueble que haya sido objeto de dicha declaración y que ésta los reconozca como parte esencial de su historia.

Artículo veintiocho.

1. Los bienes muebles declarados de interés cultural y los incluidos en el Inventario General que estén en posesión de instituciones eclesiásticas, en cualquiera de sus establecimientos o dependencias, no podrán transmitirse por título oneroso o gratuito ni cederse a particulares ni a entidades mercantiles. Dichos bienes sólo podrán ser enajenados o cedidos al Estado, a entidades de Derecho Público o a otras instituciones eclesiásticas.

2. Los bienes muebles que forman parte del Patrimonio Histórico Español no podrán ser enajenados por las Administraciones Públicas, salvo las transmisiones que entre sí mismas éstas efectúen y lo dispuesto en los artículos 29 y 34 de esta Ley.

3. Los bienes a que se refiere este artículo serán imprescriptibles. En ningún caso se aplicará a estos bienes lo dispuesto en el artículo 1.955 del Código Civil.

Artículo veintinueve.

1. Pertenecen al Estado los bienes muebles integrantes del Patrimonio Histórico Español que sean exportados sin la autorización requerida por el artículo 5.º de esta Ley. Dichos bienes son inalienables e imprescriptibles.

2. Corresponde a la Administración del Estado realizar los actos conducentes a la total recuperación de los bienes ilegalmente exportados.

3. Cuando el anterior titular acreditase la pérdida o sustracción previa del bien ilegalmente exportado, podrá solicitar su cesión del Estado, obligándose a abonar el importe de los gastos derivados de su recuperación, y, en su caso, el reembolso del precio que hubiere satisfecho el Estado al adquirente de buena fe. Se presumirá la pérdida o sustracción del bien ilegalmente exportado cuando el anterior titular fuera una Entidad de derecho público.

4. Los bienes recuperados y no cedidos serán destinados a un centro público, previo informe del Consejo del Patrimonio Histórico.

Artículo treinta.

La autorización para la exportación de cualquier bien mueble integrante del Patrimonio Histórico Español estará sujeta a una tasa establecida de acuerdo con las siguientes reglas:

A) Hecho imponible: Lo constituirá la concesión de la autorización de exportación de los mencionados bienes.

B) Exenciones: Estarán exentas del pago de las tasas:

1. La exportación de bienes muebles que tenga lugar durante los diez años siguientes a su importación, siempre que ésta se hubiere realizado de forma legal, esté reflejada documentalmente y los bienes no hayan sido declarados de interés cultural de acuerdo con lo dispuesto en el artículo 32 de esta Ley.

2. La salida temporal legalmente autorizada de bienes muebles que formen parte del Patrimonio Histórico Español.

3. La exportación de objetos muebles de autores vivos.

C) Sujeto pasivo: Estarán obligadas al pago de la tasa las personas o entidades nacionales o extranjeras a cuyo favor se concedan las autorizaciones de exportación.

D) Base imponible: La base imponible vendrá determinada por el valor real del bien cuya autorización de exportación se solicita. Se considerará valor real del bien el declarado por el solicitante, sin perjuicio de la comprobación administrativa realizada por el Organismo correspondiente de la Administración del Estado, que prevalecerá cuando sea superior a aquél.

E) Tipo de gravamen: La tasa se exigirá conforme a la siguiente tarifa:

Hasta 1.000.000 de pesetas, el 5 por 100.
De 1.000.001 a 10.000.000, el 10 por 100.
De 10.000.001 a 100.000.000, el 20 por 100.
De 100.000.001 en adelante, el 30 por 100.

F) Devengo: Se devengará la tasa cuando se conceda la autorización de exportación.

G) Liquidación y pago: El Gobierno regulará los procedimientos de valoración, liquidación y pago de la tasa.

H) Gestión: La gestión de esta tasa quedará atribuida al Ministerio de Cultura.

I) Destino: El producto de esta tasa se ingresará en el Tesoro Público, quedando afectado exclusivamente a la adquisición de bienes de interés para el Patrimonio Histórico Español.

Artículo treinta y uno.

1. La Administración del Estado podrá autorizar la salida temporal de España, en la forma y condiciones que reglamentariamente se determine, de bienes muebles sujetos al régimen previsto en el artículo 5.º de esta Ley. En todo caso deberá constar en la autorización el plazo y garantías de la exportación. Los bienes así exportados no podrán ser objeto del ejercicio del derecho de preferente adquisición.

2. El incumplimiento de las condiciones para el retorno a España de los bienes que de ese modo se hayan exportado tendrá consideración de exportación ilícita.

Artículo treinta y dos.

1. Los bienes muebles cuya importación haya sido realizada legalmente y esté debidamente documentada, de modo que el bien importado quede plenamente identificado, no podrán ser declarados de interés cultural en un plazo de diez años a contar desde la fecha de su importación.

2. Tales bienes podrán exportarse previa licencia de la Administración del Estado, que se concederá siempre que la solicitud cumpla los requisitos exigidos por la legislación en vigor, sin que pueda ejercitarse derecho alguno de preferente adquisición respecto de ellos. Antes de que finalice el plazo de diez años los poseedores de dichos bienes podrán solicitar de la Administración del Estado prorrogar esta situación, que se concederá siempre que la solicitud cumpla los requisitos exigidos por la legislación en vigor y oído el dictamen de la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español.

Las prórrogas del régimen especial de la importación regulado en este artículo se concederán tantas veces como sean solicitadas, en los mismos términos y con idénticos requisitos que la primera prórroga.

Por el contrario, si los poseedores de dichos bienes no solicitan, en tiempo y forma, prorrogar el régimen de importación, dichos bienes quedarán sometidos al régimen general de la presente ley.

3. No obstante lo dispuesto en los apartados anteriores, los bienes muebles que posean alguno de los valores señalados en el artículo 1.º de esta Ley podrán ser declarados de interés cultural antes del plazo de diez años si su propietario solicitase dicha declaración y la Administración del Estado resolviera que el bien enriquece el Patrimonio Histórico Español.

4. Lo dispuesto en los apartados 1 y 2 de este artículo no será aplicable a las adquisiciones de bienes del Patrimonio Histórico Español realizadas fuera del territorio español para su importación al mismo que se acojan a las deducciones previstas en el

artículo 55, apartado 5, párrafo a), de la Ley 40/1998, de 9 de diciembre, del Impuesto sobre la Renta de las Personas Físicas y otras Normas Tributarias, y en el artículo 35, apartado 1, párrafo a), de la Ley 43/1995, de 27 de diciembre, del Impuesto sobre Sociedades.

Artículo treinta y tres.

Salvo lo previsto en el artículo 32, siempre que se formule solicitud de exportación, la declaración de valor hecha por el solicitante será considerada oferta de venta irrevocable en favor de la Administración del Estado que, de no autorizar dicha exportación, dispondrá de un plazo de seis meses para aceptar la oferta y de un año a partir de ella para efectuar el pago que proceda. La negativa a la solicitud de exportación no supone la aceptación de la oferta, que siempre habrá de ser expresa.

Artículo treinta y cuatro.

El Gobierno podrá concertar con otros Estados la permuta de bienes muebles de titularidad estatal pertenecientes al Patrimonio Histórico Español por otros de al menos igual valor y significado histórico. La aprobación precisará de informe favorable de las Reales Academias de la Historia y de Bellas Artes de San Fernando y de la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español.

TITULO IV

Sobre la protección de los bienes muebles e inmuebles

Artículo treinta y cinco.

1. Para la protección de los bienes integrantes del Patrimonio Histórico Español y al objeto de facilitar el acceso de los ciudadanos a los mismos, fomentar la comunicación entre los diferentes servicios y promover la información necesaria para el desarrollo de la investigación científica y técnica se formularán periódicamente Planes Nacionales de Información sobre el Patrimonio Histórico Español.

2. El Consejo del Patrimonio Histórico Español elaborará y aprobará los Planes Nacionales de Información referidos en el apartado anterior.

3. Los diferentes servicios públicos y los titulares de bienes del Patrimonio Histórico Español deberán prestar su colaboración en la ejecución de los Planes Nacionales de Información.

Artículo treinta y seis.

1. Los bienes integrantes del Patrimonio Histórico Español deberán ser conservados, mantenidos y custodiados por sus propietarios o, en su caso, por los titulares de derechos reales o por los poseedores de tales bienes.

2. La utilización de los bienes declarados de interés cultural, así como de los bienes muebles incluidos en el Inventario General, quedará subordinada a que no se pongan en peligro los valores que aconsejen su conservación. Cualquier cambio de uso deberá ser autorizado por los Organismos competentes para la ejecución de esta Ley.

3. Cuando los propietarios o los titulares de derechos reales sobre bienes declarados de interés cultural o bienes incluidos en el Inventario General no ejecuten las actuaciones exigidas en el cumplimiento de la obligación prevista en el apartado 1.º de este artículo, la Administración competente, previo requerimiento a los interesados, podrá ordenar su ejecución subsidiaria. Asimismo, podrá conceder una ayuda con carácter de anticipo reintegrable que, en caso de bienes inmuebles, será inscrita en el Registro de la Propiedad. La Administración competente también podrá realizar de modo directo las obras necesarias, si así lo requiere la más eficaz conservación de los bienes. Excepcionalmente la Administración competente podrá ordenar el depósito de los bienes muebles en centros de carácter público en tanto no desaparezcan las causas que originaron dicha necesidad.

4. El incumplimiento de las obligaciones establecidas en el presente artículo será causa de interés social para la expropiación forzosa de los bienes declarados de interés cultural por la Administración competente.

Artículo treinta y siete.

1. La Administración competente podrá impedir un derribo y suspender cualquier clase de obra o intervención en un bien declarado de interés cultural.

2. Igualmente podrá actuar de ese modo, aunque no se haya producido dicha declaración, siempre que aprecie la concurrencia de alguno de los valores a que hace mención el artículo 1.º de esta Ley. En tal supuesto la Administración resolverá en el plazo máximo de treinta días hábiles en favor de la continuación de la obra o intervención iniciada o procederá a incoar la declaración de Bien de Interés Cultural.

3. Será causa justificativa de interés social para la expropiación por la Administración competente de los bienes afectados por una declaración de interés cultural el peligro de destrucción o deterioro, o un uso incompatible con sus valores. Podrán expropiarse por igual causa los inmuebles que impidan o perturben la contemplación de los bienes afectados por la declaración de interés cultural o den lugar a riesgos para los mismos. Los Municipios podrán acordar también la expropiación de tales bienes notificando previamente este propósito a la Administración competente, que tendrá prioridad en el ejercicio de esta potestad.

Artículo treinta y ocho.

1. Quien tratare de enajenar un bien declarado de interés cultural o incluido en el Inventario General al que se refiere el artículo 26 deberá notificarlo a los Organismos mencionados en el artículo 6.º y declarar el precio y condiciones en que se proponga realizar la enajenación. Los subastadores deberán notificar igualmente y con suficiente antelación las subastas públicas en que se pretenda enajenar cualquier bien integrante del Patrimonio Histórico Español.

2. Dentro de los dos meses siguientes a la notificación referida en el apartado anterior, la Administración del Estado podrá hacer uso del derecho de tanteo para sí, para una entidad benéfica o para cualquier entidad de derecho público, obligándose al pago del precio convenido, o, en su caso, el de remate en un período no superior a dos ejercicios económicos, salvo acuerdo con el interesado en otra forma de pago.

3. Cuando el propósito de enajenación no se hubiera notificado correctamente la Administración del Estado podrá ejercer, en los mismos términos previstos para el derecho de tanteo, el de retracto en el plazo de seis meses a partir de la fecha en que tenga conocimiento fehaciente de la enajenación.

4. Lo dispuesto en los apartados anteriores no excluye que los derechos de tanteo y retracto sobre los mismos bienes puedan ser ejercidos en idénticos términos por los demás Organismos competentes para la ejecución de esta Ley. No obstante, el ejercicio de tales derechos por parte de la Administración del Estado tendrá carácter preferente siempre que se trate de adquirir bienes muebles para un Museo, Archivo o Biblioteca de titularidad estatal.

5. Los Registradores de la Propiedad y Mercantiles no inscribirán documento alguno por el que se transmita la propiedad o cualquier otro derecho real sobre los bienes a que hace referencia este artículo sin que se acredite haber cumplido cuantos requisitos en él se recogen.

Artículo treinta y nueve.

1. Los poderes públicos procurarán por todos los medios de la técnica la conservación, consolidación y mejora de los bienes declarados de interés cultural, así como de los bienes muebles incluidos en el Inventario General a que alude el artículo 26 de esta Ley. Los bienes declarados de interés cultural no podrán ser sometidos a tratamiento alguno sin autorización expresa de los Organismos competentes para la ejecución de la Ley.

2. En el caso de bienes inmuebles, las actuaciones a que se refiere el párrafo anterior irán encaminadas a su conservación, consolidación y rehabilitación y evitarán los intentos de

reconstrucción, salvo cuando se utilicen partes originales de los mismos y pueda probarse su autenticidad. Si se añadiesen materiales o partes indispensables para su estabilidad o mantenimiento, las adiciones deberán ser reconocibles y evitar las confusiones miméticas.

3. Las restauraciones de los bienes a que se refiere el presente artículo respetarán las aportaciones de todas las épocas existentes. La eliminación de alguna de ellas sólo se autorizará con carácter excepcional y siempre que los elementos que traten de suprimirse supongan una evidente degradación del bien y su eliminación fuere necesaria para permitir una mejor interpretación histórica del mismo. Las partes suprimidas quedarán debidamente documentadas.

TITULO V

Del Patrimonio Arqueológico

Artículo cuarenta.

1. Conforme a lo dispuesto en el artículo 1.º de esta Ley, forman parte del Patrimonio Histórico Español los bienes muebles o inmuebles de carácter histórico, susceptibles de ser estudiados con metodología arqueológica, hayan sido o no extraídos y tanto si se encuentran en la superficie o en el subsuelo, en el mar territorial o en la plataforma continental. Forman parte, asimismo, de este Patrimonio los elementos geológicos y paleontológicos relacionados con la historia del hombre y sus orígenes y antecedentes.

2. Quedan declarados Bienes de Interés Cultural por ministerio de esta Ley las cuevas, abrigos y lugares que contengan manifestaciones de arte rupestre.

Artículo cuarenta y uno.

1. A los efectos de la presente Ley son excavaciones arqueológicas las remociones en la superficie, en el subsuelo o en los medios subacuáticos que se realicen con el fin de descubrir e investigar toda clase de restos históricos o paleontológicos, así como los componentes geológicos con ellos relacionados.

2. Son prospecciones arqueológicas las exploraciones superficiales o subacuáticas, sin remoción del terreno, dirigidas al estudio, investigación o examen de datos sobre cualquiera de los elementos a que se refiere el apartado anterior.

3. Se consideran hallazgos casuales los descubrimientos de objetos y restos materiales que, poseyendo los valores que son propios del Patrimonio Histórico Español, se hayan producido por azar o como consecuencia de cualquier otro tipo de remociones de tierra, demoliciones u obras de cualquier índole.

Artículo cuarenta y dos.

1. Toda excavación o prospección arqueológica deberá ser expresamente autorizada por la Administración competente, que, mediante los procedimientos de inspección y control idóneos, comprobará que los trabajos estén planteados y desarrollados conforme a un programa detallado y coherente que contenga los requisitos concernientes a la conveniencia, profesionalidad e interés científico.

2. La autorización para realizar excavaciones o prospecciones arqueológicas obliga a los beneficiarios a entregar los objetos obtenidos, debidamente inventariados, catalogados y acompañados de una Memoria, al Museo o centro que la Administración competente determine y en el plazo que se fije, teniendo en cuenta su proximidad al lugar del hallazgo y las circunstancias que hagan posible, además de su adecuada conservación, su mejor función cultural y científica. En ningún caso será de aplicación a estos objetos lo dispuesto en el artículo 44.3 de la presente Ley.

3. Serán ilícitas y sus responsables serán sancionados conforme a lo dispuesto en la presente Ley, las excavaciones o prospecciones arqueológicas realizadas sin la autorización correspondiente, o las que se hubieren llevado a cabo con incumplimiento de los términos en que fueron autorizadas, así como las obras de remoción de tierra, de demolición o cualesquiera otras realizadas con posterioridad en el lugar donde se haya producido un

hallazgo casual de objetos arqueológicos que no hubiera sido comunicado inmediatamente a la Administración competente.

Artículo cuarenta y tres.

La Administración competente podrá ordenar la ejecución de excavaciones o prospecciones arqueológicas en cualquier terreno público o privado del territorio español, en el que se presuma la existencia de yacimientos o restos arqueológicos, paleontológicos o de componentes geológicos con ellos relacionados. A efectos de la correspondiente indemnización regirá lo dispuesto en la legislación vigente sobre expropiación forzosa.

Artículo cuarenta y cuatro.

1. Son bienes de dominio público todos los objetos y restos materiales que posean los valores que son propios del Patrimonio Histórico Español y sean descubiertos como consecuencia de excavaciones, remociones de tierra u obras de cualquier índole o por azar. El descubridor deberá comunicar a la Administración competente su descubrimiento en el plazo máximo de treinta días e inmediatamente cuando se trate de hallazgos casuales. En ningún caso será de aplicación a tales objetos lo dispuesto en el artículo 351 del Código Civil.
2. Una vez comunicado el descubrimiento, y hasta que los objetos sean entregados a la Administración competente, al descubridor le serán de aplicación las normas del depósito legal, salvo que los entregue a un Museo público.
3. El descubridor y el propietario del lugar en que hubiere sido encontrado el objeto tienen derecho, en concepto de premio en metálico, a la mitad del valor que en tasación legal se le atribuya, que se distribuirá entre ellos por partes iguales. Si fuesen dos o más los descubridores o los propietarios se mantendrá igual proporción.
4. El incumplimiento de las obligaciones previstas en los apartados 1 y 2 de este artículo privará al descubridor y, en su caso, al propietario del derecho al premio indicado y los objetos quedarán de modo inmediato a disposición de la Administración competente, todo ello sin perjuicio de las responsabilidades a que hubiere lugar y las sanciones que procedan.
5. Se exceptúa de lo dispuesto en este artículo el hallazgo de partes integrantes de la estructura arquitectónica de un inmueble incluido en el Registro de Bienes de Interés Cultural. No obstante el hallazgo deberá ser notificado a la Administración competente en un plazo máximo de treinta días.

Artículo cuarenta y cinco.

Los objetos arqueológicos adquiridos por los Entes Públicos por cualquier título se depositarán en los Museos o Centros que la Administración adquirente determine, teniendo en cuenta las circunstancias referidas en el artículo 42, apartado 2, de esta Ley.

TITULO VI

Del Patrimonio Etnográfico

Artículo cuarenta y seis.

Forman parte del Patrimonio Histórico Español los bienes muebles e inmuebles y los conocimientos y actividades que son o han sido expresión relevante de la cultura tradicional del pueblo español en sus aspectos materiales, sociales o espirituales.

Artículo cuarenta y siete.

1. Son bienes inmuebles de carácter etnográfico, y se regirán por lo dispuesto en los títulos II y IV de la presente Ley, aquellas edificaciones e instalaciones cuyo modelo constitutivo sea expresión de conocimientos adquiridos, arraigados y transmitidos consuetudinariamente y cuya factura se acomode, en su conjunto o parcialmente, a una clase, tipo o forma arquitectónicos utilizados tradicionalmente por las comunidades o grupos humanos.

2. Son bienes muebles de carácter etnográfico, y se regirán por lo dispuesto en los títulos III y IV de la presente Ley, todos aquellos objetos que constituyen la manifestación o el producto de actividades laborales, estéticas y lúdicas propias de cualquier grupo humano, arraigadas y transmitidas consuetudinariamente.

3. Se considera que tienen valor etnográfico y gozarán de protección administrativa aquellos conocimientos o actividades que procedan de modelos o técnicas tradicionales utilizados por una determinada comunidad. Cuando se trate de conocimientos o actividades que se hallen en previsible peligro de desaparecer, la Administración competente adoptará las medidas oportunas conducentes al estudio y documentación científicos de estos bienes.

TITULO VII

Del Patrimonio Documental y Bibliográfico y de los Archivos, Bibliotecas y Museos

CAPITULO I

Del Patrimonio Documental y Bibliográfico

Artículo cuarenta y ocho.

1. A los efectos de la presente Ley forma parte del Patrimonio Histórico Español el Patrimonio Documental y Bibliográfico, constituido por cuantos bienes, reunidos o no en Archivos y Bibliotecas, se declaren integrantes del mismo en este capítulo.

2. El Patrimonio Documental y Bibliográfico se regulará por las normas específicas contenidas en este Título. En lo no previsto en ellas le será de aplicación cuanto se dispone con carácter general en la presente Ley y en su régimen de bienes muebles.

Artículo cuarenta y nueve.

1. Se entiende por documento, a los efectos de la presente Ley, toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos. Se excluyen los ejemplares no originales de ediciones.

2. Forman parte del Patrimonio Documental los documentos de cualquier época generados, conservados o reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público, por las personas jurídicas en cuyo capital participe mayoritariamente el Estado u otras entidades públicas y por las personas privadas, físicas o jurídicas, gestoras de servicios públicos en lo relacionado con la gestión de dichos servicios.

3. Forman igualmente parte del Patrimonio Documental los documentos con una antigüedad superior a los cuarenta años generados, conservados o reunidos en el ejercicio de sus actividades por las entidades y asociaciones de carácter político, sindical o religioso y por las entidades, fundaciones y asociaciones culturales y educativas de carácter privado.

4. Integran asimismo el Patrimonio Documental los documentos con una antigüedad superior a los cien años generados, conservados o reunidos por cualesquiera otras entidades particulares o personas físicas.

5. La Administración del Estado podrá declarar constitutivos del Patrimonio Documental aquellos documentos que, sin alcanzar la antigüedad indicada en los apartados anteriores, merezcan dicha consideración.

Artículo cincuenta.

1. Forman parte del Patrimonio Bibliográfico las bibliotecas y colecciones bibliográficas de titularidad pública y las obras literarias, históricas, científicas o artísticas de carácter unitario o seriado, en escritura manuscrita o impresa, de las que no conste la existencia de al menos tres ejemplares en las bibliotecas o servicios públicos. Se presumirá que existe este número de ejemplares en el caso de obras editadas a partir de 1958.

2. Asimismo forman parte del Patrimonio Histórico Español y se les aplicará el régimen correspondiente al Patrimonio Bibliográfico los ejemplares producto de ediciones de

películas cinematográficas, discos, fotografías, materiales audiovisuales u otros similares, cualquiera que sea su soporte material, de las que no consten al menos tres ejemplares en los servicios públicos, o uno en el caso de películas cinematográficas.

Artículo cincuenta y uno.

1. La Administración del Estado, en colaboración con las demás Administraciones competentes, confeccionará el Censo de los bienes integrantes del Patrimonio Documental y el Catálogo colectivo de los bienes integrantes del Patrimonio Bibliográfico conforme a lo que se determine reglamentariamente.

2. A los efectos previstos en el apartado anterior, la Administración competente podrá recabar de los titulares de derechos sobre los bienes integrantes del Patrimonio Documental y Bibliográfico el examen de los mismos, así como las informaciones pertinentes para su inclusión, si procede, en dichos Censo y Catálogo.

Artículo cincuenta y dos.

1. Todos los poseedores de bienes del Patrimonio Documental y Bibliográfico están obligados a conservarlos, protegerlos, destinarlos a un uso que no impida su conservación y mantenerlos en lugares adecuados.

2. Si los obligados incumplen lo dispuesto en el apartado anterior, la Administración competente adoptará las medidas de ejecución oportunas, conforme a lo previsto en el artículo 36.3 de la presente Ley. El incumplimiento de dichas obligaciones, cuando además sea desatendido el requerimiento por la Administración, podrá ser causa de interés social para la expropiación forzosa de los bienes afectados.

3. Los obligados a la conservación de los bienes constitutivos del Patrimonio Documental y Bibliográfico deberán facilitar la inspección por parte de los organismos competentes para comprobar la situación o estado de los bienes y habrán de permitir el estudio por los investigadores, previa solicitud razonada de éstos. Los particulares podrán excusar el cumplimiento de esta última obligación, en el caso de que suponga una intromisión en su derecho a la intimidad personal y familiar y a la propia imagen, en los términos que establece la legislación reguladora de esta materia.

4. La obligación de permitir el estudio por los investigadores podrá ser sustituida por la Administración competente, mediante el depósito temporal del bien en un Archivo, Biblioteca o Centro análogo de carácter público que reúna las condiciones adecuadas para la seguridad de los bienes y su investigación.

Artículo cincuenta y tres.

Los bienes integrantes del Patrimonio Documental y Bibliográfico, que tengan singular relevancia, serán incluidos en una sección especial del Inventario General de bienes muebles del Patrimonio Histórico Español, conforme al procedimiento establecido en el artículo 26 de esta Ley.

Artículo cincuenta y cuatro.

1. Quienes por la función que desempeñen tengan a su cargo documentos a los que se refiere el artículo 49.2 de la presente Ley están obligados, al cesar en sus funciones, a entregarlos al que les sustituya en las mismas o remitirlos al Archivo que corresponda.

2. La retención indebida de los documentos a que se refiere el apartado anterior por personas o instituciones privadas dará lugar a que la Administración que los hubiera conservado, generado o reunido ordene el traslado de tales bienes a un Archivo público, sin perjuicio de la responsabilidad en que pudiera haberse incurrido.

Artículo cincuenta y cinco.

1. La exclusión o eliminación de bienes del Patrimonio Documental y Bibliográfico contemplados en el artículo 49.2 y de los demás de titularidad pública deberá ser autorizada por la Administración competente.

2. En ningún caso se podrán destruir tales documentos en tanto subsista su valor probatorio de derechos y obligaciones de las personas o los entes públicos.

3. En los demás casos la exclusión o eliminación deberá ser autorizada por la Administración competente a propuesta de sus propietarios o poseedores, mediante el procedimiento que se establecerá por vía reglamentaria.

Artículo cincuenta y seis.

1. Los actos de disposición, exportación e importación de bienes constitutivos del Patrimonio Documental y Bibliográfico quedarán sometidos a las disposiciones contenidas en el artículo 5.º y títulos III y IV de la presente Ley que les sean de aplicación.

2. En todo caso, cuando tales bienes sean de titularidad pública serán inexportables, salvo lo previsto en los artículos 31 y 34 de esta Ley.

Artículo cincuenta y siete.

1. La consulta de los documentos constitutivos del Patrimonio Documental Español a que se refiere el artículo 49.2 se atendrá a las siguientes reglas:

a) Con carácter general, tales documentos, concluida su tramitación y depositados y registrados en los Archivos centrales de las correspondientes entidades de Derecho Público, conforme a las normas que se establezcan por vía reglamentaria, serán de libre consulta a no ser que afecten a materias clasificadas de acuerdo con la Ley de Secretos Oficiales o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la defensa del Estado o la averiguación de los delitos.

b) No obstante lo dispuesto en el párrafo anterior, cabrá solicitar autorización administrativa para tener acceso a los documentos excluidos de consulta pública. Dicha autorización podrá ser concedida, en los casos de documentos secretos o reservados, por la Autoridad que hizo la respectiva declaración, y en los demás casos por el Jefe del Departamento encargado de su custodia.

c) Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos.

2. Reglamentariamente se establecerán las condiciones para la realización de la consulta de los documentos a que se refiere este artículo, así como para la obtención de reproducciones de los mismos.

Artículo cincuenta y ocho.

El estudio y dictamen de las cuestiones relativas a la calificación y utilización de los documentos de la Administración del Estado y del sector público estatal, así como su integración en los Archivos y el régimen de acceso e inutilidad administrativa de tales documentos, corresponderá a una Comisión Superior Calificadora de Documentos Administrativos, cuya composición, funcionamiento y competencias específicas se establecerán por vía reglamentaria. Asimismo podrán constituirse Comisiones Calificadoras en los Organismos públicos que así se determine.

CAPITULO II

De los Archivos, Bibliotecas y Museos

Artículo cincuenta y nueve.

1. Son Archivos los conjuntos orgánicos de documentos, o la reunión de varios de ellos, reunidos por las personas jurídicas públicas o privadas, en el ejercicio de sus actividades, al servicio de su utilización para la investigación, la cultura, la información y la gestión

administrativa. Asimismo, se entienden por Archivos las instituciones culturales donde se reúnen, conservan, ordenan y difunden para los fines anteriormente mencionados dichos conjuntos orgánicos.

2. Son Bibliotecas las instituciones culturales donde se conservan, reúnen, seleccionan, inventarian, catalogan, clasifican y difunden conjuntos o colecciones de libros, manuscritos y otros materiales bibliográficos o reproducidos por cualquier medio para su lectura en sala pública o mediante préstamo temporal, al servicio de la educación, la investigación, la cultura y la información.

3. Son Museos las instituciones de carácter permanente que adquieren, conservan, investigan, comunican y exhiben para fines de estudio, educación y contemplación conjuntos y colecciones de valor histórico, artístico, científico y técnico o de cualquier otra naturaleza cultural.

Artículo sesenta.

1. Quedarán sometidos al régimen que la presente Ley establece para los Bienes de Interés Cultural los inmuebles destinados a la instalación de Archivos, Bibliotecas y Museos de titularidad estatal, así como los bienes muebles integrantes del Patrimonio Histórico Español en ellos custodiados.

2. A propuesta de las Administraciones competentes el Gobierno podrá extender el régimen previsto en el apartado anterior a otros Archivos, Bibliotecas y Museos.

3. Los Organismos competentes para la ejecución de esta Ley velarán por la elaboración y actualización de los catálogos, censos y ficheros de los fondos de las instituciones a que se refiere este artículo.

Artículo sesenta y uno.

1. La Administración del Estado podrá crear, previa consulta con la Comunidad Autónoma correspondiente, cuantos Archivos, Bibliotecas y Museos considere oportunos, cuando las necesidades culturales y sociales así lo requieran y sin perjuicio de la iniciativa de otros organismos, instituciones o particulares.

2. Los Archivos, Bibliotecas y Museos de titularidad estatal y carácter nacional serán creados mediante Real Decreto.

3. La Administración del Estado promoverá la comunicación y coordinación de todos los Archivos, Bibliotecas y Museos de titularidad estatal existentes en el territorio español. A tal fin podrá recabar de ellos cuanta información considere adecuada, así como inspeccionar su funcionamiento y tomar las medidas encaminadas al mejor cumplimiento de sus fines, en los términos que, en su caso, dispongan los convenios de gestión con las Comunidades Autónomas.

Artículo sesenta y dos.

La Administración del Estado garantizará el acceso de todos los ciudadanos españoles a los Archivos, Bibliotecas y Museos de titularidad estatal, sin perjuicio de las restricciones que, por razón de la conservación de los bienes en ellos custodiados o de la función de la propia institución, puedan establecerse.

Artículo sesenta y tres.

1. Los Archivos, Bibliotecas y Museos de titularidad estatal podrán admitir en depósito bienes de propiedad privada o de otras administraciones públicas de acuerdo con las normas que por vía reglamentaria se establezcan.

2. Los Bienes de Interés Cultural, así como los integrantes del Patrimonio Documental y Bibliográfico custodiados en Archivos y Museos de titularidad estatal no podrán salir de los mismos sin previa autorización, que deberá concederse mediante Orden ministerial. Cuando se trate de objeto en depósito se respetará lo pactado al constituirse.

3. El mismo régimen previsto en el apartado anterior se aplicará a los Bienes de Interés Cultural custodiados en Bibliotecas de titularidad estatal, sin perjuicio de lo que se establezca sobre servicios de préstamos públicos.

Artículo sesenta y cuatro.

Los edificios en que estén instalados Archivos, Bibliotecas y Museos de titularidad pública, así como los edificios o terrenos en que vayan a instalarse, podrán ser declarados de utilidad pública a los fines de su expropiación. Esta declaración podrá extenderse a los edificios o terrenos contiguos cuando así lo requieran razones de seguridad para la adecuada conservación de los inmuebles o de los bienes que contengan.

Artículo sesenta y cinco.

1. Cada Departamento ministerial asegurará la coordinación del funcionamiento de todos los Archivos del Ministerio y de los Organismos a él vinculados para el mejor cumplimiento de lo preceptuado en la presente Ley y en los Reglamentos que se dicten para su aplicación.
2. La documentación de los Organismos dependientes de la Administración del Estado será regularmente transferida, según el procedimiento que por vía reglamentaria se establezca a los Archivos del Estado.

Artículo sesenta y seis.

Constituyen los Sistemas Españoles de Archivos, de Bibliotecas y de Museos, respectivamente, los Archivos, Bibliotecas y Museos, así como los servicios de carácter técnico o docente directamente relacionados con los mismos, que se incorporen en virtud de lo que se disponga reglamentariamente.

TITULO VIII

De las medidas de fomento

Artículo sesenta y siete.

El Gobierno dispondrá las medidas necesarias para que la financiación de las obras de conservación, mantenimiento y rehabilitación, así como de las prospecciones y excavaciones arqueológicas realizadas en bienes declarados de interés cultural tengan preferente acceso al crédito oficial en la forma y con los requisitos que establezcan sus normas reguladoras. A tal fin, la Administración del Estado podrá establecer, mediante acuerdos con personas y Entidades públicas y privadas, las condiciones para disfrutar de los beneficios crediticios.

Artículo sesenta y ocho.

1. En el presupuesto de cada obra pública, financiada total o parcialmente por el Estado, se incluirá una partida equivalente al menos al 1 por 100 de los fondos que sean de aportación estatal con destino a financiar trabajos de conservación o enriquecimiento del Patrimonio Histórico Español o de fomento de la creatividad artística, con preferencia en la propia obra o en su inmediato entorno.

Téngase en cuenta que el artículo tercero de la Ley 14/2021, de 11 de octubre, Ref. BOE-A-2021-16477 añade un art. 1 bis al Real Decreto-ley 17/2020, de 5 de mayo, con el siguiente tenor:

«De acuerdo con lo establecido en el artículo 68.1 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, y el Real Decreto 111/1986, de 10 de enero, de desarrollo parcial de la misma, que establecen que en el presupuesto de cada obra pública, financiada total o parcialmente por el Estado, se destinará una partida de los fondos que sean de aportación estatal, a la financiación de trabajos de conservación o enriquecimiento del Patrimonio Histórico Español, o de fomento de la creatividad artística. Este porcentaje pasa a ser del 2% y para ello se modificará el Sexto Acuerdo entre el Ministerio de Fomento y el Ministerio de Educación, Cultura y Deporte que estableció el último porcentaje, así como las modificaciones presupuestarias que resulten necesarias, de conformidad con lo establecido en la Ley 47/2003, de 26 de noviembre, General Presupuestaria.»

2. Si la obra pública hubiera de construirse y explotarse por particulares en virtud de concesión administrativa y sin la participación financiera del Estado, el 1 por 100 se aplicará sobre el presupuesto total para su ejecución.

3. Quedan exceptuadas de lo dispuesto en los anteriores apartados las siguientes obras públicas:

a) Aquéllas cuyo presupuesto total no exceda de cien millones de pesetas.

b) Las que afecten a la seguridad y defensa del Estado, así como a la seguridad de los servicios públicos.

4. Por vía reglamentaria se determinará el sistema de aplicación concreto de los fondos resultantes de la consignación del 1 por 100 a que se refiere este artículo.

Artículo sesenta y nueve.

1. Como fomento al cumplimiento de los deberes y en compensación a las cargas que en esta Ley se imponen a los titulares o poseedores de los bienes integrantes del Patrimonio Histórico Español, además de las exenciones fiscales previstas en las disposiciones reguladoras de la Contribución Territorial Urbana y del Impuesto Extraordinario sobre el Patrimonio de las Personas Físicas, se establecen los beneficios fiscales fijados en los artículos siguientes.

2. Para disfrutar de tales beneficios, salvo el establecido en el artículo 72.1, los bienes afectados deberán ser inscritos previamente en el Registro General que establece el artículo 12, en el caso de Bienes de Interés Cultural, y en el Inventario General a que se refieren los artículos 26 y 53, en el caso de bienes muebles. En el caso de Conjuntos Históricos, Sitios Históricos o Zonas Arqueológicas, sólo se considerarán inscritos los inmuebles comprendidos en ellos que reúnan las condiciones que reglamentariamente se establezcan.

3. En los términos que establezcan las Ordenanzas Municipales, los bienes inmuebles declarados de interés cultural quedarán exentos del pago de los restantes impuestos locales que graven la propiedad o se exijan por su disfrute o transmisión, cuando sus propietarios o titulares de derechos reales hayan emprendido o realizado a su cargo obras de conservación, mejora o rehabilitación en dichos inmuebles.

4. En ningún caso procederá la compensación con cargo a los Presupuestos Generales del Estado en favor de los Ayuntamientos interesados.

Artículo setenta.

1. Los contribuyentes del Impuesto sobre la Renta de las Personas Físicas tendrán derecho a una deducción sobre la cuota equivalente al 20 por 100 de las inversiones que realicen en la adquisición, conservación, reparación, restauración, difusión y exposición de bienes declarados de interés cultural, en las condiciones que por vía reglamentaria se señalen. El importe de la deducción en ningún caso podrá exceder del 30 por 100 de la base imponible.

2. Asimismo, los contribuyentes de dicho impuesto tendrán derecho a deducir de la cuota el 20 por 100 de las donaciones puras y simples que hicieren en bienes que formen parte del Patrimonio Histórico Español siempre que se realizaren en favor del Estado y demás Entes públicos, así como de las que se lleven a cabo en favor de establecimientos, instituciones, fundaciones o asociaciones, incluso las de hecho de carácter temporal, para arbitrar fondos, clasificadas o declaradas benéficas o de utilidad pública por los Organos competentes del Estado, cuyos cargos de patronos, representantes legales o gestores de hecho sean gratuitos, y se rindan cuentas al órgano de protectorado correspondiente. La base de esta deducción no podrá exceder del 30 por 100 de la base imponible.

Artículo setenta y uno.

(Derogado)

Artículo setenta y dos.

1. Quedan exentas del pago del Impuesto sobre el Lujo y del Impuesto sobre el Tráfico de Empresas las adquisiciones de obras de arte siempre que sus autores vivan en el momento de la transmisión.

2. Quedan exentas de todo tributo las importaciones de bienes muebles que sean incluidos en el Inventario o declarados de interés cultural conforme a los artículos 26.3 y 32.3, respectivamente. La solicitud presentada a tal efecto por sus propietarios, en el momento de la importación, tendrá efectos suspensivos de la deuda tributaria.

Artículo setenta y tres.

El pago de las deudas Tributarias podrá efectuarse mediante la entrega de bienes que formen parte del Patrimonio Histórico Español, que estén inscritos en el Registro General de Bienes de Interés Cultural o incluidos en el Inventario General, en los términos y condiciones previstos reglamentariamente.

Artículo setenta y cuatro.

Las valoraciones necesarias para la aplicación de las medidas de fomento que se establecen en el presente título se efectuarán en todo caso por la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español, en los términos y conforme al procedimiento que se determine por vía reglamentaria. En el supuesto del artículo anterior, las valoraciones citadas no vincularán al interesado, que podrá optar por el pago en metálico.

TITULO IX

De las infracciones administrativas y sus sanciones

Artículo setenta y cinco.

1. La exportación de un bien mueble integrante del Patrimonio Histórico Español que se realice sin la autorización prevista en el artículo 5.º de esta Ley constituirá delito, o en su caso, infracción de contrabando, de conformidad con la legislación en esta materia. Serán responsables solidarios de la infracción o delito cometido cuantas personas hayan intervenido en la exportación del bien y aquellas otras que por su actuación u omisión, dolosa o negligente, la hubieren facilitado o hecho posible.

2. La fijación del valor de los bienes exportados ilegalmente se realizará por la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español, dependiente de la Administración del Estado, cuya composición y funciones se establecerán por vía reglamentaria.

Artículo setenta y seis.

1. Salvo que sean constitutivos de delito, los hechos que a continuación se mencionan constituyen infracciones administrativas que serán sancionadas conforme a lo dispuesto en este artículo:

a) El incumplimiento por parte de los propietarios o de los titulares de derechos reales o los poseedores de los bienes de las disposiciones contenidas en los artículos 13, 26.2, 4 y 6, 28, 35.3, 36.1 y 2, 38.1, 39, 44, 51.2 y 52.1 y 3.

b) La retención ilícita o depósito indebido de documentos según lo dispuesto en el artículo 54.1.

c) El otorgamiento de licencias para la realización de obras que no cumpla lo dispuesto en el artículo 23.

d) La realización de obras en Sitios Históricos o Zonas Arqueológicas sin la autorización exigida por el artículo 22.

e) La realización de cualquier clase de obra o intervención que contravenga lo dispuesto en los artículos 16, 19, 20, 21, 25, 37 y 39.

f) La realización de excavaciones arqueológicas u otras obras ilícitas a que se refiere el artículo 42.3.

g) El derribo, desplazamiento o remoción ilegales de cualquier inmueble afectado por un expediente de declaración de Bien de Interés Cultural.

h) La exportación ilegal de los bienes a que hacen referencia los artículos 5.º y 56.1 de la presente Ley.

i) El incumplimiento de las condiciones de retorno fijadas para la exportación temporal legalmente autorizada.

j) La exclusión o eliminación de bienes del Patrimonio Documental y Bibliográfico que contravenga lo dispuesto en el artículo 55.

2. Cuando la lesión al Patrimonio Histórico Español ocasionada por las infracciones a que se refiere el apartado anterior sea valorable económicamente, la infracción será sancionada con multa del tanto al cuádruplo del valor del daño causado.

3. En los demás casos se impondrán las siguientes sanciones:

A) Multa de hasta 60.101,21 euros en los supuestos a) y b) del apartado 1.

B) Multa de hasta 150.253,03 euros en los supuestos c), d), e) y f) del apartado 1.

C) Multa de hasta 601.012,10 euros en los supuestos g), h), i) y j) del apartado 1.

Artículo setenta y siete.

1. Las sanciones administrativas requerirán la tramitación de un expediente con audiencia del interesado para fijar los hechos que las determinen y serán proporcionales de la gravedad de los mismos, a las circunstancias personales del sancionado y al perjuicio causado o que pudiera haberse causado al Patrimonio Histórico Español.

2. Las multas que se impongan a distintos sujetos como consecuencia de una misma infracción tendrán carácter independiente entre sí.

Artículo setenta y ocho.

Las multas de hasta 150.253,03 euros serán impuestas por los Organismos competentes para la ejecución de esta Ley. Las de cuantía superior a 150.253,03 euros serán impuestas por el Consejo de Ministros o los Consejos de Gobierno de las Comunidades Autónomas.

Artículo setenta y nueve.

1. Las infracciones administrativas contra lo dispuesto en esta Ley prescribirán a los cinco años de haberse cometido, salvo las contenidas en los apartados g), h), i) y j) del artículo 76.1, que prescribirán a los diez años.

2. En todo lo no previsto en el presente título será de aplicación el Capítulo II del Título VI de la Ley de Procedimiento Administrativo.

Disposición adicional primera.

Los bienes que con anterioridad hayan sido declarados histórico-artísticos o incluidos en el Inventario del Patrimonio Artístico y Arqueológico de España pasan a tener la consideración y a denominarse Bienes de Interés Cultural; los muebles que hayan sido declarados integrantes del Tesoro o incluidos en el Inventario del Patrimonio Histórico-Artístico tienen la condición de bienes inventariados conforme al artículo 26 de esta Ley, sin perjuicio de su posible declaración expresa como Bienes de Interés Cultural. Todos ellos quedan sometidos al régimen jurídico que para esos bienes la presente Ley establece.

Disposición adicional segunda.

Se consideran asimismo de Interés Cultural y quedan sometidos al régimen previsto en la presente Ley los bienes a que se contraen los Decretos de 22 de abril de 1949, 571/1963 y 499/1973(*).

(*) Entendemos que se refiere al Decreto 449/1973.

Disposición adicional tercera.

1. Los documentos del Inventario del Patrimonio Artístico y Arqueológico de España se incorporarán al Registro General al que se refiere el artículo 12 de esta Ley.

2. Los documentos del Inventario del Tesoro Artístico Nacional se incorporarán al Inventario General de bienes muebles previsto en el artículo 26.

3. Asimismo, los documentos propios del Censo-Guía de Archivos se incorporarán al Censo del Patrimonio Documental, y los del Catálogo General del Tesoro Bibliográfico pasarán al Catálogo Colectivo.

4. Por la Dirección General de Bellas Artes y Archivos se procederá a la integración de los documentos a que se refieren los apartados precedentes en el plazo de un año a partir de la entrada en vigor de la presente Ley.

Disposición adicional cuarta.

La exigencia a que se refiere el artículo 69.2 de la presente Ley obligará igualmente a los titulares de los bienes señalados en el artículo 6, j), de la Ley 50/1977, de 14 de noviembre, sobre Medidas Urgentes de Reforma Fiscal, para beneficiarse de la exención que en el mismo se prevé. La misma exigencia se incorpora a las establecidas en el Real Decreto 1382/1978, de 2 de junio, en el que la referencia al Inventario contenida en su artículo 2.º queda suprimida.

Disposición adicional quinta.

Quedan sujetos a cuanto se dispone en esta Ley cuantos bienes muebles e inmuebles formen parte del Patrimonio Nacional y puedan incluirse en el ámbito del artículo 1.o, sin perjuicio de su afectación y régimen jurídico propio.

Disposición adicional sexta.

El Gobierno negociará en los correspondientes Acuerdos, Convenios y Tratados Internacionales cláusulas tendentes a reintegrar al territorio español los bienes culturales que hayan sido exportados ilegalmente.

Disposición adicional séptima.

Sin perjuicio de lo dispuesto en la presente Ley, las Administraciones a quienes corresponda su aplicación quedarán también sujetas a los Acuerdos Internacionales válidamente celebrados por España. La actividad de tales Administraciones estará asimismo encaminada al cumplimiento de las resoluciones y recomendaciones que para la protección del Patrimonio Histórico adopten los Organismos Internacionales de los que España sea miembro.

Disposición adicional octava.

La aceptación de donaciones, herencias o legados a favor del Estado, aunque se señale como beneficiario a algún otro órgano de la Administración, relativos a toda clase de bienes que constituyan expresión o testimonio de la creación humana y tengan un valor cultural, bien sea de carácter histórico, artístico, científico o técnico, corresponderá al Ministerio de Cultura, entendiéndose aceptada la herencia a beneficio de inventario.

Corresponderá asimismo a dicho Ministerio aceptar análogas donaciones en metálico que se efectúen con el fin específico y concreto de adquirir, restaurar o mejorar alguno de dichos bienes. El importe de esta donación se ingresará en el Tesoro Público y generará crédito en el concepto correspondiente del presupuesto del Ministerio de Cultura.

Por el Ministerio de Cultura se informará al Ministerio de Economía y Hacienda de las donaciones, herencias o legados que se acepten conforme a lo dispuesto en los párrafos anteriores.

Disposición adicional novena.

1. El Estado podrá comprometerse a indemnizar por la destrucción, pérdida, sustracción o daño de aquellas obras de relevante interés artístico, histórico, paleontológico, arqueológico, etnográfico, científico o técnico que se cedan temporalmente para su exhibición pública a museos, bibliotecas o archivos de titularidad estatal y competencia exclusiva del Ministerio de Educación, Cultura y Deporte y sus organismos públicos adscritos.

2. A los efectos de esta disposición, la Fundación Colección Thyssen-Bornemisza tendrá la misma consideración que los museos señalados en el párrafo anterior.

3. El otorgamiento del compromiso del Estado se acordará para cada caso por el Ministro de Cultura a solicitud de la entidad cesionaria.

En dicho acuerdo se precisará la obra u obras a que se refiere, la cuantía, los requisitos de seguridad y protección exigidos y las obligaciones que deban ser cumplidas por los interesados.

El límite máximo del compromiso que se otorgue a una obra o conjunto de obras para su exhibición en una misma exposición así como el límite del importe total acumulado de los compromisos otorgados por el Estado se establecerán en las leyes anuales de Presupuestos Generales del Estado.

4. Por Real Decreto, a propuesta de los Ministros de Cultura, y de Economía y Hacienda, se regulará el procedimiento y requisitos para el otorgamiento de este compromiso y la forma de hacerlo efectivo en su caso.

Disposición adicional décima. *Arrendamiento de colecciones de bienes muebles integrantes del Patrimonio Histórico Español por determinadas entidades del sector público.*

1. El arrendamiento, con o sin opción de compra, por parte de las entidades del sector público que, con arreglo al artículo 3 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, tengan la consideración de poder adjudicador no Administración Pública, de colecciones de bienes muebles integrantes del Patrimonio Histórico Español cuyo interés excepcional haya sido declarado por la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español, u órgano equivalente de las comunidades autónomas, tendrá naturaleza de contrato privado; y su preparación y adjudicación se regirán por lo dispuesto en el artículo 26 de la Ley 9/2017, de 8 de noviembre.

En cuanto a sus efectos y extinción, con carácter general les serán aplicables las normas de derecho privado. No obstante, cuando el contrato tenga la consideración de contrato sujeto a regulación armonizada con arreglo a lo previsto en la Ley 9/2017, de 8 de noviembre, le será aplicable lo dispuesto en el párrafo segundo del artículo 26.3 de dicha ley, salvo las normas relativas a la racionalización técnica de la contratación. Asimismo, no será obligatorio el establecimiento de condiciones especiales de ejecución, pero, de incorporarse, en todo caso deberán estar vinculadas al objeto del contrato, en el sentido del artículo 145.6 de la Ley 9/2017, de 8 de noviembre, no serán directa o indirectamente discriminatorias, serán compatibles con el Derecho de la Unión Europea y se indicarán en el expediente de la contratación.

No obstante, no resultarán de aplicación los siguientes preceptos de la Ley 9/2017, de 8 de noviembre:

a) El artículo 29, relativo al plazo de duración de los contratos y de ejecución de la prestación. En estos contratos, el plazo de duración será como máximo de 15 años.

b) El capítulo II del título III del libro I, relativo a la revisión de precios de los contratos de las entidades del sector público, así como lo dispuesto en la Ley 2/2015, de 30 de marzo, de desindexación de la economía española.

En los contratos a los que se refiere esta disposición, excepcionalmente, cuando la duración sea superior a 5 años, podrá preverse la revisión anual periódica y predeterminada del precio. Esta revisión en ningún caso podrá conllevar incrementos de la renta superiores al índice de precios al consumo del correspondiente año.

c) Los artículos 198.4 y 210.4, relativos a las condiciones especiales de pago.

Asimismo, el pago de cada anualidad de renta podrá efectuarse de forma anticipada, sin que resulte exigible ningún otro requisito adicional.

La resolución de controversias sobre los efectos y extinción del contrato podrá encomendarse a una Comisión mixta, compuesta por representantes de los arrendadores y de la entidad del sector público arrendataria. Si transcurrido un mes dicha Comisión no lograra un acuerdo, podrá acudirse a la jurisdicción civil.

2. Al arrendamiento de estos bienes se le podrá aplicar el procedimiento negociado sin publicidad correspondiente a aquellos supuestos en los que la ejecución solo puede encomendarse a un empresario determinado, previsto en el artículo 168.a) 2.º de la Ley 9/2017, de 8 de noviembre, previa acreditación de que no existen alternativas equivalentes y de los demás requisitos exigidos al efecto, con las siguientes especialidades respecto de lo establecido en la Ley 9/2017, de 8 de noviembre:

a) En estos contratos, el pliego de cláusulas administrativas particulares será sustituido por el propio clausulado del contrato, sin perjuicio de la obligación del órgano de contratación de elaborar el correspondiente expediente; así como el informe previsto en el artículo 336 de la Ley 9/2017, 8 de noviembre, en el caso de contratos sujetos a regulación armonizada.

b) La acreditación de la titularidad de los bienes, o de otro derecho real que permita ceder su uso, así como de los requisitos de capacidad del arrendador, se realizará conforme a las normas de derecho privado aplicables. La solvencia se entenderá justificada con la acreditación de la titularidad de las obras o del derecho real que permita ceder su uso.

c) En el caso de que la colección de bienes muebles esté integrada por un conjunto de obras que pertenezcan a más de un titular, podrán concurrir todos ellos conjuntamente a la licitación, previa acreditación de dicha titularidad, sin necesidad de constituir una unión de empresarios. Esta misma previsión será aplicable a los supuestos en que sean varios los titulares de cualesquiera otros derechos que permitan ceder el uso de las obras que integran la colección.

Cada uno de los titulares deberá tener plena capacidad de obrar y no estar incurso en ninguna prohibición de contratar.

Los titulares quedarán obligados solidariamente y deberán nombrar un representante para ejercitar los derechos y cumplir las obligaciones que del contrato se deriven hasta la extinción del mismo.

Disposición adicional undécima. *Adquisición por las entidades del sector público de bienes muebles integrantes del Patrimonio Histórico Español.*

1. Con independencia de los procedimientos para el ejercicio de los derechos de adquisición preferente previstos en los artículos 33 y 38 de la presente ley, la adquisición por parte de las entidades del sector público de bienes muebles integrantes del Patrimonio Histórico Español tendrá naturaleza de contrato privado; y su preparación y adjudicación se regirán por lo dispuesto en el artículo 26 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

En cuanto a sus efectos y extinción, con carácter general les serán aplicables las normas de derecho privado. No obstante, cuando el contrato merezca la consideración de contrato sujeto a regulación armonizada con arreglo a lo previsto en la Ley 9/2017, de 8 de noviembre, le será aplicable, según proceda, lo dispuesto en el párrafo segundo del apartado 2 del artículo 26 o en el párrafo segundo del apartado 3 del artículo 26 de dicha Ley, salvo las normas relativas a la racionalización técnica de la contratación.

2. A las adquisiciones de estos bienes se les podrá aplicar el procedimiento negociado sin publicidad correspondiente a aquellos supuestos en los que la ejecución solo puede encomendarse a un empresario determinado, previsto en el artículo 168.a) 2.º de la Ley 9/2017, de 8 de noviembre, según lo indicado en los apartados 3 y 4 de esta disposición, con las siguientes especialidades respecto de lo establecido en la Ley 9/2017, de 8 de noviembre:

a) En estos contratos, el pliego de cláusulas administrativas particulares será sustituido por el propio clausulado del contrato.

b) Podrá aplazarse el pago del precio convenido en varios ejercicios económicos si así se acuerda con el interesado.

c) La acreditación de la titularidad de los bienes, así como de los requisitos de capacidad del vendedor, se realizará conforme a las normas de derecho privado aplicables, no siendo necesario acreditar su solvencia, excepto cuando se trate de contratos sujetos a regulación armonizada de acuerdo con lo establecido en la Ley 9/2017, de 8 de noviembre.

3. Cuando las adquisiciones de bienes del Patrimonio Histórico se destinen a museos, archivos o bibliotecas de titularidad estatal o autonómica, solo podrán realizarse si cuentan, respectivamente, con informe previo favorable emitido por la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español o del organismo equivalente reconocido al efecto de la Comunidad Autónoma titular del archivo, biblioteca o museo destinatario del bien.

Dichos informes deberán hacer referencia al precio de compra, a la pertenencia del bien al patrimonio histórico español, conforme a la definición del mismo del artículo 1.2 de esta ley, y a la unicidad del bien, a los efectos previstos en el artículo 168.a) 2.° de la Ley 9/2017, de 8 de noviembre, como requisito inexcusable para la aplicación del procedimiento previsto en esta disposición.

4. En los expedientes de adquisición de bienes de esta naturaleza destinados a instituciones diferentes de las contempladas en el apartado anterior y que por tanto no hayan sido informadas por la Junta de Calificación, Valoración y Exportación de Bienes del Patrimonio Histórico Español u organismo equivalente reconocido al efecto de las Comunidades Autónomas, además de la condición de bien del patrimonio histórico y la disponibilidad de crédito, deberá justificarse la oportunidad de la compra, incorporando la correspondiente memoria, valoración económica e informe técnico, que incluirá la Motivación de la unicidad en los términos previstos en el apartado anterior.

5. Cuando no concurran los requisitos previstos en los apartados 3 y 4, la adquisición se regulará por lo dispuesto en la Ley 9/2017, de 8 de noviembre.

Disposición transitoria primera.

En tanto se elaboran las normas precisas para el desarrollo y aplicación de la presente Ley, se entenderán vigentes las de rango reglamentario que regulan el Patrimonio Histórico-Artístico Español, el Tesoro Documental y Bibliográfico, los Archivos, Bibliotecas y Museos, en todo aquello que no contravenga lo dispuesto en la misma.

Disposición transitoria segunda.

En el plazo de un año a partir de la entrada en vigor de la presente Ley, el Gobierno, a propuesta del Ministerio de Cultura, dictará el Reglamento de organización, funcionamiento y personal de los Archivos, Bibliotecas y Museos de titularidad estatal, así como de los servicios técnicos o docentes relacionados con ellos o con las actividades que competen a la Administración del Estado en la protección del Patrimonio Histórico Español.

Disposición transitoria tercera.

Quienes a la entrada en vigor de la presente Ley fuesen propietarios, poseedores o tenedores de algunos de los bienes a que se refieren los artículos 26 y 53 de la presente Ley dispondrán del plazo de un año para comunicar la existencia de dichos bienes a la Administración competente. En tal caso, la citada comunicación determinará la exención, en relación a tales bienes, de cualesquiera impuestos o gravámenes no satisfechos con anterioridad, así como de toda responsabilidad frente a la Hacienda Pública o los restantes Organos de la Administración por incumplimientos, sanciones, recargos o intereses de demora.

Disposición transitoria cuarta.

(Derogada)

Disposición transitoria quinta.

En los diez años siguientes a la entrada en vigor de esta Ley, lo dispuesto en el artículo 28.1 de la misma se entenderá referido a los bienes muebles integrantes del Patrimonio Histórico Español en posesión de las instituciones eclesiásticas.

Téngase en cuenta que se amplía por cinco años el plazo previsto en esta Ley en relación con el Inventario de Bienes Muebles de la Iglesia, y en relación a su vez con esta disposición, a partir del 30 de abril de 2021, según establece la disposición adicional única de la Ley 6/2021, de 28 de abril. Ref. BOE-A-2021-6945

Disposición transitoria sexta.

1. La tramitación y efectos de los expedientes sobre declaración de bienes inmuebles de valor histórico-artístico incoados con anterioridad a la entrada en vigor de esta Ley se regirán por la normativa en virtud de la cual han sido iniciados, pero su resolución se efectuará en todo caso mediante Real Decreto, y con arreglo a las categorías previstas en el artículo 14.2 de la presente Ley.

2. En los Conjuntos Históricos ya declarados que dispongan de un Plan Especial de Protección u otro instrumento de planeamiento del área afectada por la declaración, aprobado con anterioridad a la entrada en vigor de esta Ley, la autorización de obras se regirá por lo dispuesto en el artículo 20.3 hasta que no se haya obtenido de la Administración competente el informe favorable sobre el instrumento de planeamiento a aplicar. A estos efectos se entenderá emitido informe favorable transcurrido un año desde la presentación del Plan sin que haya recaído resolución expresa.

Disposición transitoria séptima.

En el plazo de cinco años a partir de la entrada en vigor de la Ley, los responsables de la instalación deberán retirar la publicidad comercial, así como los cables y conducciones a que se refiere el artículo 19.3.

Disposición transitoria octava.

Los Parajes Pintorescos a que se refiere la disposición transitoria de la Ley 15/1975, de 2 de mayo, de Espacios Naturales Protegidos, mientras no sean reclasificados conforme a su disposición final, conservarán la condición de Bienes de Interés Cultural.

Disposición final.

1. Se autoriza al Gobierno para dictar, además de las disposiciones reglamentarias expresamente previstas en la presente Ley, las que sean precisas para su cumplimiento.

2. El Gobierno queda, asimismo, autorizado para proceder por vía reglamentaria a la actualización de la cuantía de las multas que se fijan en el artículo 76 de la presente Ley, sin que los porcentajes de los incrementos que por tal vía se establezcan puedan ser superiores, en ningún caso, al Indice Oficial del Coste de Vida.

3. La Ley de Presupuestos Generales del Estado podrá determinar anualmente las fórmulas de actualización de la base imponible y de los tipos de gravamen de la tasa por exportación a que se refiere el artículo 30.

4. Se autoriza también al Gobierno para que, a iniciativa del Ministerio de Cultura y a propuesta del Ministerio del Interior, disponga la creación en los Cuerpos y Fuerzas de Seguridad del Estado de un Grupo de Investigación formado por personal especializado en las materias que son objeto de la presente Ley y destinado a perseguir sus infracciones.

Disposición derogatoria.

1. Quedan derogadas la Ley de 7 de julio de 1911 sobre Excavaciones Arqueológicas; el Real Decreto-Ley de 9 de agosto de 1926 sobre Protección, Conservación y

Acrecentamiento de la Riqueza Artística; la Ley de 10 de diciembre de 1931 sobre enajenación de bienes artísticos, arqueológicos e históricos de más de cien años de antigüedad; la Ley de 13 de mayo de 1933 sobre defensa, conservación y acrecentamiento del Patrimonio Histórico Artístico; la Ley de 22 de diciembre de 1955 sobre Conservación del Patrimonio Histórico Artístico; el Decreto 1641/1959, de 23 de septiembre, sobre exportación de objetos de valor e interés arqueológico o artístico y de imitaciones o copias, y la Ley 26/1972, de 21 de junio, sobre Defensa del Tesoro Documental y Bibliográfico de la Nación, salvo las disposiciones relativas al Centro Nacional del Tesoro Documental y Bibliográfico, las cuales, no obstante, tendrán en adelante rango reglamentario, y el Real Decreto 2832/1978, de 28 de octubre, sobre el 1 por 100 cultural.

2. Asimismo quedan derogadas cuantas disposiciones se opongan a lo establecido en la presente Ley.

Información relacionada

- Sentencia del TC 17/1991, de 31 de enero . Ref. BOE-T-1991-5257l

§ 26

Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso. [Inclusión parcial]

Ministerio de la Presidencia
«BOE» núm. 284, de 25 de noviembre de 2011
Última modificación: 16 de febrero de 2022
Referencia: BOE-A-2011-18541

[. . .]

CAPÍTULO III

Sistema de Archivos de la Administración General del Estado y de sus organismos públicos

[. . .]

Sección 4.ª Documentos electrónicos y preservación digital.

Artículo 20. *Condiciones para la recuperación y conservación del documento electrónico.*

1. Las disposiciones del presente Real Decreto relativas a los documentos integrantes del Sistema de Archivos de la Administración General del Estado, serán de aplicación también a los documentos en soporte electrónico, con las especialidades derivadas de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, de los Esquemas Nacionales de Seguridad e Interoperabilidad, y demás normativa de desarrollo.

2. Los Departamentos Ministeriales y las entidades de derecho público vinculadas o dependientes de los mismos, adoptarán las decisiones organizativas y las medidas técnicas necesarias con el fin de garantizar la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Entre éstas:

a) La identificación clara y precisa de cada uno de los documentos mediante un código unívoco que permita su identificación en un entorno de intercambio interadministrativo.

b) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios asociados al documento electrónico.

c) La inclusión, en el caso de los expedientes electrónicos, de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del mismo y permita su recuperación.

d) La recuperación completa e inmediata de los documentos a través de métodos de consulta en línea a los datos que permita la visualización de los documentos de modo que sean legibles e identificables.

e) La adopción de medidas para garantizar la conservación de la memoria e identificación de los órganos que ejercen la competencia sobre el documento o expediente para que el ciudadano de hoy y del futuro pueda comprender el contexto en el que se creó.

f) El mantenimiento del valor probatorio de los documentos y expedientes y de las evidencias electrónicas como prueba de las actividades y procedimientos, así como la observancia de las obligaciones jurídicas que incumban a los servicios.

g) La transferencia de los expedientes electrónicos a los archivos históricos para la conservación permanente, de acuerdo con lo establecido en la normativa vigente, de manera que se pueda asegurar su conservación y accesibilidad a medio y largo plazo.

h) El borrado de la información, en su caso, o si procede la destrucción física de los soportes, de acuerdo con un procedimiento regulado y dejando registro de su eliminación.

i) La valoración y el establecimiento de las estrategias que se pueden aplicar para la conservación a medio y largo plazo de los documentos, tales como procedimientos de emulación, migración y conversión de formatos.

Artículo 21. *Aplicación de las tecnologías de la información y comunicaciones en la gestión y tratamiento de los documentos.*

Los Departamentos Ministeriales y sus organismos vinculados o dependientes promoverán en todo momento el uso de las tecnologías de la información y el conocimiento en el tratamiento archivístico de los documentos de su competencia y en todo lo relativo a las funciones de conservación, gestión, acceso y difusión que tiene encomendadas, mediante:

a) La utilización de sistemas de gestión, de acuerdo con los requisitos establecidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y su normativa de desarrollo.

b) El desarrollo de archivos digitales o repositorios de documentos en soporte electrónico estableciendo formatos de intercambio de documentos o expedientes electrónicos definiendo unos metadatos y clasificaciones comunes que permitan la reutilización y el intercambio de información entre los distintos órganos de la Administración.

c) La aplicación de los principios básicos y los requisitos mínimos requeridos para una protección adecuada de la información con el fin de asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

d) El desarrollo de Sistemas Integrales de Información y Gestión de Archivos y su implementación en plataformas informáticas compartidas, con procedimientos de actualización en línea y accesibles por Internet.

e) La implantación progresiva de los servicios telemáticos que permitan recoger, gestionar y dar respuesta al conjunto de solicitudes, reclamaciones y sugerencias que realicen los ciudadanos sobre acceso, localización, reproducción, u otras cuestiones relacionadas con los documentos o los servicios que prestan los archivos del Sistema.

Artículo 22. *Documentos en formato electrónico transferidos al Archivo Intermedio de la Administración General del Estado.*

Las decisiones organizativas y medidas técnicas previstas en este capítulo no supondrán para la documentación transferida al Archivo Intermedio de la Administración General del Estado por los distintos Ministerios y Organismos, obligaciones adicionales a las previstas en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en los Esquemas Nacionales de Seguridad e Interoperabilidad y demás normativa de desarrollo.

[. . .]

§ 27

Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 262, de 31 de octubre de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-13501

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, el Catálogo de estándares persigue facilitar que los servicios de Administración Electrónica puedan prestarse en condiciones que permitan la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas, así como la adaptabilidad al progreso de las técnicas y sistemas de comunicaciones descrito en la Ley 11/2007. Su desarrollo responde a las condiciones establecidas en el Real Decreto 4/2010, de 8 de enero, sobre estándares aplicables y se ciñe estrictamente a la finalidad de encontrarse al servicio de la interoperabilidad.

Para este fin, la Norma Técnica de Interoperabilidad de Catálogo de estándares establece un catálogo formado por un conjunto mínimo de estándares que satisfacen lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero, y que dan soporte al resto de Normas Técnicas de Interoperabilidad; asimismo establece condiciones necesarias para su revisión y actualización. Atendiendo a lo anterior, el uso de estándares no incluidos en esta norma respondería a necesidades específicas que igualmente aplicarían lo establecido en dicho artículo 11.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Catálogo de estándares cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Catálogo de estándares que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE CATÁLOGO DE ESTÁNDARES

I. Objeto

La Norma Técnica de Interoperabilidad de Catálogo de estándares tiene por objeto establecer un conjunto de estándares que satisfagan lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

II. Ámbito de aplicación

Esta norma será de aplicación en el ámbito establecido en el artículo 3 del citado Real Decreto 4/2010, de 8 de enero.

III. Catálogo de estándares

El Catálogo de estándares:

a) Incluirá el conjunto de estándares definido en el anexo estructurado conforme a diferentes categorías.

b) Atenderá a la aplicación de los criterios establecidos en el artículo 11 del Real Decreto 4/2010, de 8 de enero.

c) Recogerá los estándares mínimos necesarios para la interoperabilidad y para la implementación del resto de Normas Técnicas de Interoperabilidad.

d) Indicará para cada estándar el estado que le corresponde dentro del ciclo de vida, siendo los valores aplicables «Admitido» y «En abandono».

IV. Uso de los estándares

Cada órgano de la Administración o Entidad de Derecho Público vinculada o dependiente de aquella:

a) Seleccionará, entre los establecidos en esta norma, el estándar o estándares que mejor se ajuste a sus necesidades, en base a su especificidad para la tarea o funcionalidad a cubrir, para los documentos y servicios que pongan a disposición de los ciudadanos o de otras Administraciones públicas, atendiendo a las condiciones establecidas en el artículo 11 del Real Decreto 4/2010, de 8 de enero.

Si una determinada funcionalidad o necesidad no quedara cubierta por ningún estándar de los recogidos en esta norma, podrá seleccionar el estándar más adecuado para la tarea atendiendo a lo establecido en artículo 11.2 del Real Decreto 4/2010, de 8 de enero. En este caso, informará del estándar seleccionado según lo establecido en el apartado V.2 de esta norma.

b) Para la interacción con otras administraciones, atenderá a los estándares seleccionados por el emisor del documento solicitado o responsable del servicio al que se desea acceder, que éste publicará según lo establecido en el artículo 8 del Real Decreto 4/2010, de 8 de enero. Dicha selección de estándares se realizará atendiendo a las condiciones establecidas en el artículo 11 del citado Real Decreto.

c) Publicará, según lo establecido en la normativa aplicable en cada caso, los estándares seleccionados para los servicios o trámites que ponga a disposición del ciudadano.

d) Podrá utilizar otros formatos cuando existan particularidades que lo justifiquen o sea necesario para asegurar el valor probatorio de la información electrónica de las actividades y procedimientos en caso de proceder a su conversión de formato.

V. Revisión y actualización del Catálogo de estándares

1. La actualización y revisión del Catálogo de estándares se realizará con periodicidad anual, atenderá a los principios establecidos en el artículo 11 del Real Decreto 4/2010 e incluirá, al menos, las siguientes acciones:

a) Encuesta a las Administraciones públicas sobre el uso de los diferentes estándares del Catálogo.

b) Valoración y, si procede, eliminación de los estándares cuyo estado fuese «En abandono». Esta situación conllevará la selección de un estándar que sustituya la funcionalidad cubierta por el estándar eliminado.

c) Revisión del resto de estándares, así como de sus versiones, recogidos en el Catálogo a la fecha de la revisión de la misma, actualización, para aquellos que así lo requiriesen e identificación de los estándares en estado «En abandono», en cuyo caso se definirá un período máximo de uso.

d) Identificación de nuevos estándares a incluir en el Catálogo.

e) Valoración de nuevas necesidades o funcionalidades que no puedan catalogarse según la clasificación establecida y, si corresponde, modificación de las categorías y actualización del Catálogo de estándares en base a ésta.

2. En los casos necesarios, se podrá solicitar la actualización del Catálogo de estándares mediante petición formal a la Secretaría Ejecutiva del Comité Sectorial de Administración Electrónica, para decisión del mismo, que incluirá:

a) Tipo de solicitud: alta, modificación o baja de un estándar.

b) Datos a actualizar del estándar.

c) Razón de la actualización.

ANEXO

Catálogo de estándares

La tabla que figura a continuación recoge el conjunto de estándares incluidos en el Catálogo.

Para cada uno de ellos, se incluyen los siguientes atributos:

a) Cadena de interoperabilidad: eslabón de la cadena de interoperabilidad con el que se relaciona:

– Accesibilidad multicanal, integrada y segura.
– Infraestructuras y servicios asociados.
– Integración de sistemas y servicios.
– Modelos e integración de datos.

b) Categoría: Definición de la categoría funcional en la que se enmarca:

– Autenticación:

Certificados.
Firma electrónica.
Política de firma electrónica.

– Sellado de tiempo.
– Cifrado.

– Codificación:

Codificación de caracteres.
Idioma.

– Control de acceso.
– Formatos ficheros:

Imagen y/o texto.
Cartografía vectorial y sistemas de información geográfica.
Compresión de ficheros.
Contenedores multimedia.
Sonido.
Vídeo.

– Gestión documental y archivística.
– Integridad.
– Métricas.
– Protocolos de comunicación e intercambio:

Correo electrónico.
Específicos a nivel de aplicación.
Servicios Web.
Tecnologías de transporte y red.

– Semántica:

Metadatos.
Tecnologías semánticas.

– Tecnologías de integración de datos.
– Tecnologías de identificación.

c) Nombre:

– Común: nombre común por el que se conoce el estándar, normalmente identificado por su extensión. Define el valor a asignar al metadato mínimo obligatorio «Nombre de formato» de los documentos electrónicos.
– Formal: nombre correspondiente a la especificación formal del estándar.

d) Tipo:

– Estándar abierto.
– Uso generalizado.

e) Versión: versión mínima aceptada del estándar.

f) Extensión: Con carácter informativo, aproximación al listado no exhaustivo de extensiones más comunes relacionadas con el estándar.

g) Estado:

– Admitido.

– En abandono.

Cadena de Interoperabilidad	Categoría	Nombre		Tipo		Versión (mínima aceptada)	Extensión	Estado
		Común	Formal					
Accesibilidad multicanal, integrada y segura	Autenticación–Firma electrónica	CAdES	ETSI TS 101 733 Electronic Signatures and Infrastructures (ESO; CMS Advanced Electronic Signatures (CAdES)	Abierto		1.6.3	.p7s .csig	Admitido
Accesibilidad multicanal, integrada y segura.	Autenticación - Firma electrónica	CMS	Cryptographic Message Syntax (CMS)	Abierto		RFC 5652	.sig	Admitido
Accesibilidad multicanal, integrada y segura	Autenticación - Firma electrónica	ETSI TS 102 176-1	ETSI TS 102 176-1. Electronic Signatures and Infrastructures (ESI); Algorithms and parameters for secure electronic signature. Part 1: Hash functions and asymmetric algorithms	Abierto		2.0.0	–	Admitido
Accesibilidad multicanal, integrada y segura.	Autenticación - Firma electrónica	PAdES	ETSI TS 102 778-3 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.	Abierto		PAdES-1 1.1.1 PAdES-3 1.1.2 PAdES-4 1.1.2	.p7s .pdf	Admitido
Accesibilidad multicanal, integrada y segura	Autenticación - Firma electrónica	PDF Signature	PDF Signature		Uso generalizado	–	.pdf	En abandono
Accesibilidad multicanal, integrada y segura	Autenticación - Firma electrónica	PKCS#7	PKCS #7: Cryptographic Message Syntax. Version 1.5	Abierto		RFC 2315	–	En abandono
Accesibilidad multicanal, integrada y segura	Autenticación - Firma electrónica	(XAdES)	ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)	Abierto		1.2.2	.xml. .dsig .xsig	Admitido
Accesibilidad multicanal, integrada y segura	Autenticación - Firma electrónica	XML-DSig	XML Signature Syntax and Processing.	Abierto		Second edition. 2008	.xmp .dsig .xsig .sig	Admitido
Accesibilidad multicanal, integrada y segura	Autenticación - Política Firma electrónica	ETSI TR 102 038	ETS TR 102 038 TC Security - Electronic Signatures and Infrastructures (ESI);XML format for signature policies	Abierto		RFC 3125 1.1.1	–	Admitido
Accesibilidad multicanal, integrada y segura	Autenticación - Política Firma electrónica	ETS TR 102 272	ETSI TR 102 272 Electronic Signatures and Infrastructures (ESO; ASN.1 format for signature policies	Abierto		1.1.1	–	Admitido
Accesibilidad multicanal, integrada y segura	Cifrado	TLS	Transport Layer Security (TLS)	Abierto		RFC 5878 RFC 5746 RFC 5705 RFC 5489 RFC 5487 RFC 5469 RFC 5289 RFC 5288	–	Admitido
Accesibilidad multicanal, integrada y segura	Codificación-Codificación de caracteres	Base16, Base32 y Base64	The Base16, Base32, and Base64 Data Encodings	Abierto		RFC 4648	–	Admitido
Accesibilidad multicanal, integrada y segura.	Codificación - Codificación de caracteres	UCS UTF	ISO/IEC 10646:2003 Information technology - Universal Multiple-Octet Coded Character Set (UCS)	Abierto		2003	–	Admitido
Accesibilidad multicanal, integrada y segura.	Codificación idioma	RFC 4646 ISO 639	Tags for Identifying Languages. ISO 639 Codes for the representation of names of languages	Abierto		2002-2008 RFC 4646	–	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Cartografía vectorial y Sistemas de Información Geográfica	GML	IS0 19136:2007 Geographic information - Geography Markup Language (GML)	Abierto		2007	.gml	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Cartografía vectorial y Sistemas de Información Geográfica	WFS	IS0 19142:2010 Geographic information Web Feature Service	Abierto		2010	.gml	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Cartografía vectorial y Sistemas de Información Geográfica	WMS	IS0 19128:2005 Geographic information - Web map server interface	Abierto		2010	.gml	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Compresión de ficheros	GZIP	GNU Zip	Abierto		RFC 1952	.gz	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Compresión de ficheros	ZIP	ZIP RFC 1952	Abierto		–	.zip	Admitido

Cadena de Interoperabilidad	Categoría	Nombre		Tipo		Versión (mínima aceptada)	Extensión	Estado
		Común	Formal					
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Contenedores multimedia	AVI	Audio Video Interleave		Uso generalizado	–	.avi	En abandono
Accesibilidad multicanal, integrada y segura.	Formatos ficheros - Contenedores multimedia	MPEG-4 MP4 media	ISO/IEC 14496-14:2003 Information technology - Coding of audio-visual objects - Part 14: MP4 file format	Abierto		2003	mpeg .mp4	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	Comma Separated Values.	Comma Separated Values.	Abierto		RFC 4180	.csv .txt	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	HTML	HyperText Markup Language	Abierto		4.01	.html .htm	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	CSS	Cascading Style Sheets	Abierto		2.1	.css	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	JPEG	ISO/IEC 15444. Information technology - JPEG 2000 image coding system.	Abierto		2004-2008	.jpg .jpeg	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	MHTML	Multipurpose Internet Mail Extension HTML	Abierto		RFC 2557	.mhtml .mht	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	ISO/IEC 263002006 OASIS 1.2	ISO/IEC 26300:2006 Information technology - Open Document Format for Office Applications (OpenDocument) OASIS 1.2	Abierto		1.0	.odt .ods .odp .odg	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	Strict Open XML	ISO/IEC 29500-1:2012 Information technology — Document description and processing languages — Office Open XML File Formats — Part 1: Fundamentals and Markup Language Reference - Strict	Abierto		2012	.docx .xlsx .pptx	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	PDF	ISO 32000-1:2008 Document management -Portable document format - Part 1: PDF 1.7		Abierto	1.4	.pdf	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	PDFA	ISO 19005-1:2005 ISO 19005-2:2011 Document management -Electronic document file format for long-term preservation	Abierto		1.4 1.7	.pdf	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	PMG	ISO/IEC 15948:2004 Information technology - Computer graphics and image processing - Portable Network Graphics (PNG): Functional specification.	Abierto		2004	.png	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	RTF	Rich Text Format.		Uso generalizado	1.6	.rff	En abandono
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	Imagen y/o texto	SVG	Scalable Vector Graphics.	Abierto	1.1	.svg	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	TIFF	ISO 12639:2004 Graphic technology - Prepress digital data exchange - Tag image file format for image technology (TIFF/IT)	Abierto		2004	.tiff	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Imagen y/o texto	TXT	Texto plano	Abierto		–	.txt	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Sonido	MP3. MPEG-1 Audio Layer 3	ISO/IEC 11172-1:1993 ISO/IEC 11172-2:1993 ISO/IEC 11172-3:1993 ISO/IEC 11172-4:1995 ISO/IEC TR 11172-5:1998		Uso generalizado	1993-1998	.mp3	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Sonido	OGG-Vorbis	OGG Vorbis	Abierto		2010	.ogg .oga	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Vídeo	MPEG-4 MP4 Video	ISO/IEC 14496-14:2003 Information technology - Coding of audio-visual objects - Part 14: MP4 file format		Uso generalizado	2003	.mpeg .mp4	Admitido
Accesibilidad multicanal, integrada y segura.	Formatos ficheros-Vídeo	BebM	WebM	Abierto		2010	.webm	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	ISAAR CPF	International Standard Archival Autorithy Records for Corporate Bodies, Persons and Families.		Uso generalizado	–	–	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	ISAD (G)	General International Standard Archival Description.		Uso generalizado	–	–	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	ISDF	Norma internacional para la descripción de funciones.		Uso generalizado	–	–	Admitido

Cadena de Interoperabilidad	Categoría	Nombre		Tipo		Versión (mínima aceptada)	Extensión	Estado
		Común	Formal					
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	NEDA	Modelo conceptual de descripción archivística y requisitos de datos básicos de las descripciones de documentos de archivo, agentes y funciones — Parte 1: Tipos de entidad.		Uso generalizado	2007	–	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	UNE-ISO 30300	UNE-ISO 30300:2011 Información y documentación. Sistemas de gestión para los documentos. Fundamentos y vocabulario	Abierto		2011	–	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	UNE-ISO 30301	UNE-ISO 30301:2011 Información y documentación. Sistemas de gestión para los documentos. Requisitos.	Abierto		2011	–	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	UNE-ISO 15489	UNE-ISO 15489-1:2006 Parte 1: Generalidades UNE-ISOfTR 15489-2:2006. Parte 2: Directrices. (ISO/TR 15489-2:2001)	Abierto		2006	–	Admitido
Accesibilidad multicanal, integrada y segura.	Gestión documental y archivística	UNE-ISO 23081	UNE-ISO 23081-1:2008 Parte 1: Principios. UNE-ISOfTS 23081-2:2008 Parte 2: Elementos de implementación y conceptuales.	Abierto		2008	–	Admitido
Accesibilidad multicanal, integrada y segura.	Integridad	SHA	SHA	Secure Hash Algorithms	Abierto	RFC 4634 RFC 3874	–	
Infraestructuras y servicios asociados	Integridad	LDAP	Lightweight Directory Access Protocol.	Abierto		RFC 4510	–	Admitido
Infraestructuras y servicios asociados	Protocolos de comunicación e intercambio - Correo electrónico	MIME	Multipurpose Internet Mail Extensions	Abierto		RFC 2045	–	Admitido
Infraestructuras y servicios asociados	Protocolos de comunicación e intercambio - Correo electrónico	SMTP	Simple Mail Transfer Protocol	Abierto		RFC 5321	–	Admitido
Infraestructuras y servicios asociados	Protocolos de comunicación e intercambio - Tecnologías de transporte y red	DNS	Domain Name System	Abierto		RFC 1035	–	Admitido
Infraestructuras y servicios asociados	Protocolos de comunicación e intercambio - Tecnologías de transporte y red	HTTP	Hypertext Transfer Protocol	Abierto		1.1 RFC 2616 RFC 2817	http://	Admitido
Infraestructuras y servicios asociados	Protocolos de comunicación e intercambio - Tecnologías de transporte y red	IPSec	Security Architecture for the Internet Protocol	Abierto		RFC 2401 RFC 4302 RFC 4835	–	Admitido
Infraestructuras y servicios asociados	Protocolos de comunicación e intercambio - Tecnologías de transporte y red	NTP	Network Time Protocol	Abierto		RFC 5905	–	Admitido
Integración de sistemas y servicios	Autenticación - Certificados	OCSP	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP	Abierto		RFC 2560	–	Admitido
Integración de sistemas y servicios	Autenticación - Sellado de tiempo	ETSI TS 102 023	ETSI TS 102 023 Electronic Signatures and Infrastructures (ESO; Policy requirements for time-stamping authorities	Abierto		RFC 3628	–	Admitido
Integración de sistemas y servicios	Protocolos de comunicación e intercambio - Servicios Web	SOAP	Simple Object Access Protocol	Abierto		1.1	–	Admitido
Integración de sistemas y servicios	Protocolos de comunicación e intercambio - Servicios Web	UDDI	Universal Discovery, Description and Integration	Abierto		3.0	–	Admitido
Integración de sistemas y servicios	Protocolos de comunicación e intercambio - Servicios Web	WSDL	Web Services Definition Language	Abierto		1.1	–	Admitido
Integración de sistemas y servicios	Protocolos de comunicación e intercambio - Servicios Web	WS-Security	Web Services Security: SOAP Message Security	Abierto		1.1	–	Admitido
Integración de sistemas y servicios	Tecnologías para identificación	ASN.1	ISOIIEC 8824 Information technology - Abstract Syntax Notation One (ASN.1)	Abierto		2008	–	Admitido

Cadena de Interoperabilidad	Categoría	Nombre		Tipo		Versión (mínima aceptada)	Extensión	Estado
		Común	Formal					
Integración de sistemas y servicios	Tecnologías para identificación	OID	ISO/FDIS 26324 Information and documentation - Digital object identifier system	Abierto		2010	–	Admitido
Integración de sistemas y servicios	Tecnologías para identificación	URI	Uniform Resource Identifier	Abierto		RFC 3986 RFC 5785	–	Admitido
Integración de sistemas y servicios	Tecnologías para identificación	URL	Uniform Resource Locators	Abierto		RFC 1738	–	Admitido
Integración de sistemas y servicios	Tecnologías para identificación	URN	Uniform Resource Names (URN) Namespaces	Abierto		–	–	Admitido
Modelos e integración de datos.	Métricas	Fechas y horas	ISO 8601:2004 Data elements and interchange formats - Information interchange - Representation of dates and times	Abierto		2004	–	Admitido
Modelos e integración de datos.	Protocolos de comunicación e intercambio - Específicos a nivel de aplicación	CODICE	Componentes y Documentos Interoperables para la Contratación Electrónica	Abierto		2.0	.xml	Admitido
Modelos e integración de datos.	Protocolos de comunicación e intercambio - Específicos a nivel de aplicación	Facturae	Factura electrónica	Abierto		3.0	.xml	Admitido
Modelos e integración de datos.	Protocolos de comunicación e intercambio - Específicos a nivel de aplicación	SCSP	Sustitución de Certificados en papel	Abierto		2.0	–	Admitido
Modelos e integración de datos.	Protocolos de comunicación e intercambio - Específicos a nivel de aplicación	SICRES	Sistemas de Información Común de Registros de Entrada y SALIDA (SICRES)	Abierto		2.0 3.0		Admitido
Modelos e integración de datos.	Semántica	DCAT	Data Catalog Vocabulary	Abierto		–	–	Admitido
Modelos e integración de datos.	Semántica - Metadatos	MoReq	Model Requirements for the management of electronic records.	Abierto		–	–	Admitido
Modelos e integración de datos.	Semántica - Metadatos	PREMIS	PREservation Metadata: Implementation Strategies. V2.1		Uso generalizado	–	–	Admitido
Modelos e integración de datos.	Semántica - Metadatos	INSPIRE Metadata Regulation	Commission Regulation (EC) No 1205/2008 of 3 December 2008 implementing Directive 2007/2/EC of the European Parliament and of the Council as regards metadata (Text with EEA relevance)	Abierto		–		Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	N3	Notation3	Abierto		–	.n3	Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	OWL	Ontology Web Language	Abierto		2.0	–	Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	RDF	Resource Description Framework	Abierto		1.0	–	Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	RDFa	Resource Description Framework –in– attributes	Abierto		2008	–	Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	SKOS	Simple Knowledge Organization System	Abierto		2009	–	Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	SPARQL	Query Language for RDF	Abierto		2008	–	Admitido
Modelos e integración de datos.	Semántica - Tecnologías semánticas	Turtle	Terse RDF Triple Language	Abierto		2011	.ttl	Admitido
Modelos e integración de datos.	Tecnologías de integración de datos	XML	Extensible Markup Language (XML)	Abierto		1.0	.xml	Admitido
Modelos e integración de datos.	Tecnologías de integración de datos	XSD	XML Schema	Abierto		1.0	.xsd	Admitido

§ 28

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13169

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Documento electrónico establece los componentes del documento electrónico, incluyendo contenido, firma electrónica y

metadatos mínimos obligatorios, y su formato, así como las condiciones para su intercambio y reproducción; para los aspectos relativos a la gestión y conservación de los documentos electrónicos se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos; finalmente, se incluye en anexo la definición detallada de los metadatos mínimos obligatorios, los esquemas XML para intercambio de documentos y la información básica de firma de documentos electrónicos. En este sentido, la estructura de documento electrónico definida en esta norma permite la utilización de las firmas electrónicas contempladas en la Decisión de la Comisión 2011/130/EU de 25 de febrero de 2011 por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Documento electrónico, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Documento electrónico que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE DOCUMENTO ELECTRÓNICO

I. Objeto.

La Norma Técnica de Interoperabilidad de Documento electrónico tiene por objeto establecer los componentes del documento electrónico, contenido, en su caso, firma electrónica y metadatos, así como la estructura y formato para su intercambio.

II. Ámbito de aplicación.

Esta norma será de aplicación en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica a:

a) Documentos administrativos electrónicos.

b) Cualquier otro documento electrónico susceptible de formar parte de un expediente electrónico.

III. Componentes del documento electrónico.

Los componentes de un documento electrónico son:

a) Contenido, entendido como conjunto de datos o información del documento.

b) En su caso, firma electrónica.

c) Metadatos del documento electrónico.

IV. Firma del documento electrónico.

Los documentos administrativos electrónicos, y aquellos susceptibles de formar parte de un expediente, tendrán siempre asociada al menos una firma electrónica de acuerdo con la normativa aplicable.

V. Metadatos del documento electrónico.

V.1 Los metadatos mínimos obligatorios del documento electrónico:

a) Serán los definidos en el anexo I.

b) Estarán presentes en cualquier proceso de intercambio de documentos electrónicos entre órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla y con el ciudadano.

c) No serán modificados en ninguna fase posterior del procedimiento administrativo, a excepción de modificaciones necesarias para la corrección de errores u omisiones en el valor inicialmente asignado.

V.2 Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas.

Estos metadatos complementarios se aplicarán, en su caso, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

V.3 Cada órgano de la Administración y Entidad de Derecho Público vinculada o dependiente de aquélla implementará en su propio ámbito de actuación los metadatos de los documentos electrónicos para su tratamiento y gestión a nivel interno. Además, garantizará la disponibilidad e integridad de los metadatos de sus documentos electrónicos, manteniendo de manera permanente las relaciones entre el documento y sus metadatos.

VI. Formato de documentos electrónicos.

VI.1 Los ficheros de contenido de los documentos electrónicos se ajustarán a los formatos establecidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

VI.2 La elección del formato se realizará conforme a la naturaleza de la información a tratar primando la finalidad para la cual fue definido cada formato.

VI.3 Se podrán utilizar otros formatos cuando existan particularidades que lo justifiquen o sea necesario para asegurar el valor probatorio del documento electrónico y su fiabilidad como evidencia electrónica de las actividades y procedimientos en caso de proceder a su conversión de formato.

VII. Intercambio de documentos electrónicos.

VII.1 Todo documento electrónico objeto de intercambio tendrá los componentes definidos en el apartado III de esta norma.

VII.2 El intercambio de documentos electrónicos se realizará mediante su envío según la estructura definida en el anexo II, sin perjuicio de la aplicación de otras reguladas por su normativa específica.

VII.3 Excepcionalmente, se podrán aplicar otras estructuras para el intercambio de documentos electrónicos entre Administraciones públicas, cuando exista acuerdo previo entre las partes. En cualquier caso, si debe enviarse a un tercero, la estructura utilizada será convertida por el emisor a la estructura definida en el anexo II.

VII.4 Para el intercambio de documentos electrónicos, entre Administraciones públicas, en procesos de actuación automatizada:

a) Se utilizará preferentemente la Red de comunicaciones de las Administraciones públicas españolas como medio para la transmisión.

b) Si el documento electrónico forma parte de un asiento registral, éste será tratado como documento adjunto al mensaje de datos de intercambio según lo establecido en la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales.

VII.5 En caso de intercambio de documentos electrónicos entre Administraciones públicas que suponga una transferencia de custodia o traspaso de responsabilidad de gestión de documentos que deban conservarse permanentemente, el órgano o entidad trasferidora verificará la autenticidad e integridad del documento en el momento de dicho intercambio.

VIII. Acceso a documentos electrónicos.

Cuando las administraciones públicas faciliten el acceso a los documentos electrónicos a través de sus sedes electrónicas o de los canales de comunicación que correspondan en cada caso, se mostrará:

a) El contenido del documento electrónico cuando éste sea representable conforme a lo recogido sobre formatos en el apartado VI de esta norma.

b) La información básica de cada una de las firmas del documento definida en el anexo III.

c) Descripción y valor de los metadatos mínimos obligatorios.

ANEXO I

Metadatos mínimos obligatorios del documento electrónico

Metadato	Descripción/Condiciones de uso	¿Repetible?[1]	Tipo	Esquema de valores
Versión N11	Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Documento electrónico conforme a la cual se estructura el documento electrónico.	1	URI	http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e
Identificador	Identificador normalizado del documento.	1	Cadena de caracteres	ES_ <Órgano>_<AAAA>_<ID específico>[2] Ejemplo: ES E00010207 2010 MPR0000000000000000000000010207
Órgano	Identificador normalizado de la administración generadora del documento o que realiza la captura del mismo.	1:N	Cadena de caracteres	Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común gestionado por el Ministerio de Política Territorial y Administración Pública.
Fecha de captura	Fecha de alta del documento en el sistema de gestión documental.	1	Fecha/hora	Formato: AAAAMMDD T HH:MM:SS <ISO 8601>
Origen	Indica si el contenido del documento fue creado por un ciudadano o por una administración.	1	Lógico	'0' = Ciudadano '1' = Administración
Estado de elaboración	Indica la naturaleza del documento. Si es copia, este metadato indica también si se ha realizado una digitalización o conversión de formato en el proceso de generación.	1	Cadena de caracteres	– Original (Ley 11/2007 Ad. 30). – Copia electrónica auténtica con cambio de formato (Ley 11/2007Art.30.1). – Copia electrónica auténtica de documento papel (Ley 11/2007 Art.30.2 y 30.3). – Copia electrónica parcial auténtica. Otros.
Nombre de formato	Formato lógico del fichero de contenido del documento electrónico.	1	Cadena de caracteres	Valor extraído de la lista de formatos admitidos para ficheros definidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares.
				Documentos de decisión:
				– Resolución.
				– Acuerdo.
				– Contrato.
				– Convenio.
				– Declaración.
				Documentos de transmisión:
				– Comunicación.
				– Notificación.
				– Publicación.
				– Acuse de recibo.
Tipo documental	Descripción del tipo documental del documento.	1	Cadena de caracteres	Documentos de constancia:
				– Acta.
				– Certificado.
				– Diligencia.
				Documentos de juicio:
				– Informe.
				Documentos de ciudadano:
				– Solicitud.
				– Denuncia.
				– Alegación.
				– Recursos.
				– Comunicación ciudadano.
				– Factura.
				– Otros incautados.
				Otros.

Metadato	Descripción/Condiciones de uso	¿Repetible?[1]	Tipo	Esquema de valores
Tipo de firma	Indica el tipo de firma que avala el documento. En caso de firma con certificado, indica el formato de la firma.	1:N	Cadena de caracteres	– CSV – Formatos de firma electrónica de documentos electrónicos definidos en la Norma Técnica de Interoperabilidad de Política de firma y certificados de la Administración.
Si «Tipo de firma» = CSV				
Valor CSV	Valor del CSV.	1:N	Cadena de caracteres	NIA
Definición generación CSV	Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente.	1:N	Cadena de caracteres	Si AGE: Referencia BOE:BOE A YYYY-XXXXX En otro caso, referencia correspondiente.
Si «Estado de elaboración» =				
– Copia electrónica auténtica con cambio de formato (Ley 11/2007Art.30.1).				
– Copia electrónica parcial auténtica.				
Identificador de documento origen	Identificador normalizado del documento origen al que corresponde la copia.	1	Cadena de caracteres	Si el documento origen es un documento electrónico: ES_<Órgano>_<AAAA>_<ID específico> Ejemplo: ES–E00010207–2010 MPR00000000000000000000000010207

[1] Nótese que la repetibilidad indicada en la tabla sólo se refiere a los metadatos que acompañan al documento electrónico en un intercambio, sin perjuicio de la posibilidad de asignación de otros metadatos gestionados a nivel interno de cada administración cuyas consideraciones atenderán a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

[2] Codificación del Identificador del documento:

<Órgano>: Véase codificación del metadato «Órgano». En caso de más un órgano los nueve caracteres correspondientes serán acordados entre las partes con el fin de asegurarla unicidad del identificador que es su único fin.

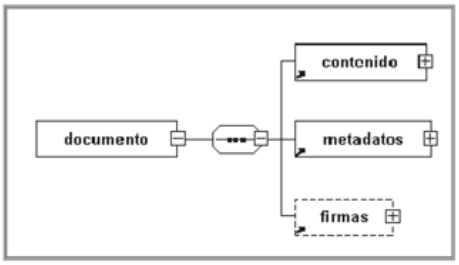
<AAAA>: Año de la fecha de captura del documento. (Longitud: 4 caracteres).

<ID específico>: Código alfanumérico que identifica de forma única al documento dentro de los generados por la administración responsable. Cada administración puede diseñar el proceso de generación según sus necesidades, asegurando en cualquier caso su unicidad. Por lo tanto, este ID puede generarse de forma secuencia) o bien, ser una réplica del ID utilizado a nivel interno de la administración. (Longitud: 30 caracteres).

ANEXO II

Esquemas XML para intercambio de documentos electrónicos

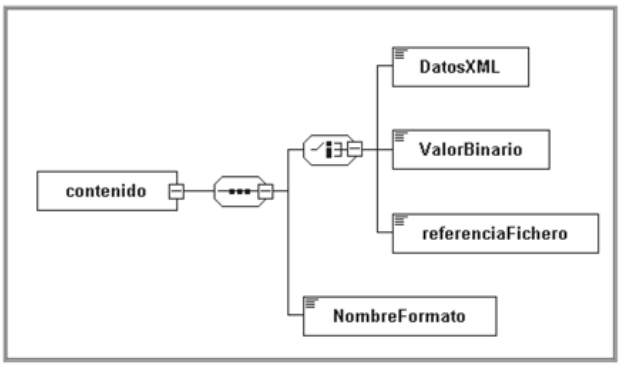
1. *XSD Documento electrónico*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:enidocmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
xmlns:enidoc="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e"
elementFormDefault="qualified" attributeFormDefault="unqualified">
    <xsd:annotation>
        <xsd:documentation xml:lang="es">XSD DOCUMENTO ENI (v1.0)</xsd:documentation>
    </xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-
e/metadatos/metadatosDocumentoEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma/firmasEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-
e/contenido/contenidoDocumentoEni.xsd"/>
<xsd:element name="documento" type="enidoc:TipoDocumento">
    <xsd:annotation>
<xsd:documentation xml:lang="es">El elemento "documento" podrá aparecer como elemento raíz de un documento XML objeto de intercambio o como elemento no raíz (elemento hijo).</xsd:documentation>
    </xsd:annotation>
</xsd:element>
<xsd:complexType name="TipoDocumento">
    <xsd:sequence>
        <xsd:element ref="enifile:contenido"/>
        <xsd:element ref="enidocmeta:metadatos"/>
        <xsd:element ref="enids:firmas" minOccurs="0" maxOccurs="1">
            <xsd:annotation>
<xsd:documentation xml:lang="es">La firma es obligatoria para el documento administrativo electrónico y para todo aquel documento electrónico susceptible de ser incorporado en un expediente
electrónico.</xsd:documentation>
            </xsd:annotation>
```

```
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

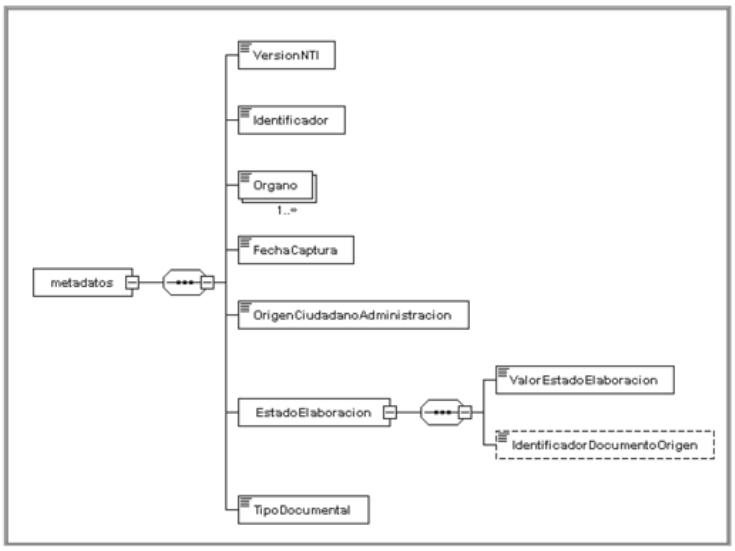
2. *XSD Contenido*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
    <xsd:documentation xml:lang="es">XSD CONTENIDO DOCUMENTO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:element name="contenido" type="enifile:TipoContenido"/>
<xsd:complexType name="TipoContenido">
    <xsd:sequence>
        <xsd:choice>
            <xsd:element name="DatosXML" type="xsd:anyType">
                <xsd:annotation>
<xsd:documentation xml:lang="es">Contenido en formato XML. En caso de datos XML cuya codificación difiera de la de esta estructura raíz se incluirá una cláusula CDATA.</xsd:documentation>
                </xsd:annotation>
            </xsd:element>
            <xsd:element name="ValorBinario" type="xsd:base64Binary">
                <xsd:annotation>
                    <xsd:documentation xml:lang="es">Contenido en base64.</xsd:documentation>
                </xsd:annotation>
            </xsd:element>
```

```
            <xsd:element name="referenciaFichero" type="xsd:string">
                <xsd:annotation>
<xsd:documentation xml:lang="es">Referencia interna al fichero de contenido. </xsd:documentation>
                </xsd:annotation>
            </xsd:element>
        </xsd:choice>
        <xsd:element name="NombreFormato" type="xsd:string">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">El formato del fichero de contenido del documento electrónico atenderá a lo establecido en la NTI de Catálogo de estándares.</xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

3. *XSD Metadatos*

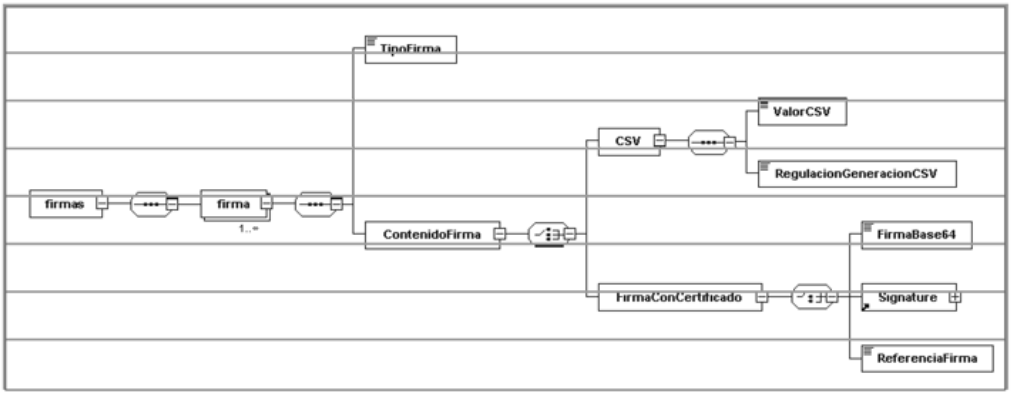


```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enidocmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/metadatos"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
     <xsd:documentation xml:lang="es">XSD METADATOS DOCUMENTO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:element name="metadatos" type="enidocmeta:TipoMetadatos"/>
<xsd:complexType name="TipoMetadatos">
     <xsd:sequence>
          <xsd:element name="VersionNTI" type="xsd:anyURI"/>
          <xsd:element name="Identificador" type="xsd:string"/>
          <xsd:element name="Organo" type="xsd:string" minOccurs="1" maxOccurs="unbounded"/>
          <xsd:element name="FechaCaptura" type="xsd:dateTime"/>
          <xsd:element name="OrigenCiudadanoAdministracion" type="xsd:boolean"/>
          <xsd:element name="EstadoElaboracion" type="enidocmeta:TipoEstadoElaboracion">
               <xsd:annotation>
                    <xsd:documentation xml:lang="es">
- EE01 - Original.
- EE02 - Copia electrónica auténtica con cambio de formato.
- EE03 - Copia electrónica auténtica de documento papel.
- EE04 - Copia electrónica parcial auténtica.
- EE99 - Otros.
                    </xsd:documentation>
               </xsd:annotation>
          </xsd:element>
          <xsd:element name="TipoDocumental" type="enidocmeta:tipoDocumental">
               <xsd:annotation>
                    <xsd:documentation xml:lang="es">/*Documentos de decisión*/
- TD01 - Resolución.
- TD02 - Acuerdo.
- TD03 - Contrato.
- TD04 - Convenio.
- TD05 - Declaración.
/*Documentos de transmisión*/
- TD06 - Comunicación.
- TD07 - Notificación.
- TD08 - Publicación.
- TD09 - Acuse de recibo.
/*Documentos de constancia*/
- TD10 - Acta.
- TD11 - Certificado.
- TD12 - Diligencia.
/*Documentos de juicio*/
- TD13 - Informe.
/*Documentos de ciudadano*/
- TD14 - Solicitud.
- TD15 - Denuncia.
- TD16 - Alegación.
```

```
- TD17 - Recursos.
- TD18 - Comunicación ciudadano.
- TD19 - Factura.
- TD20 - Otros incautados.
/*Otros*/
- TD99 - Otros.
</xsd:documentation>
                </xsd:annotation>
            </xsd:element>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
<xsd:complexType name="TipoEstadoElaboracion">
        <xsd:sequence>
            <xsd:element name="ValorEstadoElaboracion" type="enidocmeta:enumeracionEstadoElaboracion"/>
            <xsd:element name="IdentificadorDocumentoOrigen" type="xsd:string" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
</xsd:complexType>

<!-- Enumeración de estados de elaboración -->
<xsd:simpleType name="enumeracionEstadoElaboracion">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="EE01"/>
            <xsd:enumeration value="EE02"/>
            <xsd:enumeration value="EE03"/>
            <xsd:enumeration value="EE04"/>
            <xsd:enumeration value="EE99"/>
        </xsd:restriction>
</xsd:simpleType>

<!-- Enumeración de tipos documentales -->
<xsd:simpleType name="tipoDocumental">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="TD01"/>
            <xsd:enumeration value="TD02"/>
            <xsd:enumeration value="TD03"/>
            <xsd:enumeration value="TD04"/>
            <xsd:enumeration value="TD05"/>
            <xsd:enumeration value="TD06"/>
            <xsd:enumeration value="TD07"/>
            <xsd:enumeration value="TD08"/>
            <xsd:enumeration value="TD09"/>
            <xsd:enumeration value="TD10"/>
            <xsd:enumeration value="TD11"/>
            <xsd:enumeration value="TD12"/>
            <xsd:enumeration value="TD13"/>
            <xsd:enumeration value="TD14"/>
            <xsd:enumeration value="TD15"/>
            <xsd:enumeration value="TD16"/>
```

```
            <xsd:enumeration value="TD17"/>
            <xsd:enumeration value="TD18"/>
            <xsd:enumeration value="TD19"/>
            <xsd:enumeration value="TD20"/>
            <xsd:enumeration value="TD99"/>
        </xsd:restriction>
</xsd:simpleType>
</xsd:schema>
```

4. *XSD Firmas*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma "
 xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma " elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
    <xsd:documentation xml:lang="es">XSD FIRMAS ELECTRONICAS ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<xsd:element name="firmas" type="enids:firmas"/>
<xsd:complexType name="firmas">
    <xsd:sequence>
        <xsd:element name="firma" type="enids:TipoFirmasElectronicas" minOccurs="1" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="TipoFirmasElectronicas">
    <xsd:sequence>
        <xsd:element name="TipoFirma">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
```

```
                    - TF01 - CSV.
                    - TF02 - XAdES internally detached signature.
                    - TF03 - XAdES enveloped signature.
                    - TF04 - CAdES detached/explicit signature.
                    - TF05 - CAdES attached/implicit signature.
                    - TF06 - PAdES.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:simpleType>
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="TF01"/>
                    <xsd:enumeration value="TF02"/>
                    <xsd:enumeration value="TF03"/>
                    <xsd:enumeration value="TF04"/>
                    <xsd:enumeration value="TF05"/>
                    <xsd:enumeration value="TF06"/>
                </xsd:restriction>
            </xsd:simpleType>
        </xsd:element>
        <xsd:element name="ContenidoFirma">
            <xsd:complexType>
                <xsd:choice>
                    <xsd:element name="CSV">
                        <xsd:complexType>
                            <xsd:sequence>
                                <xsd:element name="ValorCSV" type="xsd:string"/>
                                <xsd:element name="RegulacionGeneracionCSV" type="xsd:string"/>
                            </xsd:sequence>
                        </xsd:complexType>
                    </xsd:element>
                    <xsd:element name="FirmaConCertificado">
                        <xsd:complexType>
                            <xsd:choice>
                                <xsd:element name="FirmaBase64" type="xsd:base64Binary"/>
                                <xsd:element ref="ds:Signature"/>
                                <xsd:element name="ReferenciaFirma">
                                    <xsd:annotation>
                                    <xsd:documentation  xml:lang="es">
                                     Referencia interna al fichero que incluye la firma.</xsd:documentation>
                                    </xsd:annotation>
                                </xsd:element>
                            </xsd:choice>
                        </xsd:complexType>
                    </xsd:element>
                </xsd:choice>
            </xsd:complexType>
        </xsd:element>
    </xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
<xsd:attribute name="ref" type="xsd:string" use="optional">

    <xsd:annotation>
        <xsd:documentation xml:lang="es">Almacena el identificador del nodo que se está firmando. En caso de firmas multinodo, se incluirá una lista separada por comas de los identificadores de los nodos
firmados.</xsd:documentation>
    </xsd:annotation>
</xsd:attribute>
</xsd:complexType>
</xsd:schema>
```

ANEXO III

Información básica de la firma de documentos electrónicos

Tipo de firma	Información	Localización
CSV	Valor del código seguro de verificación.	Metadato del documento electrónico.
Firma basada en certificados	Validez de la firma.	Según reglas de validación de firma descritas en la Norma Técnica de Interoperabilidad de Política de firma y certificados de la Administración.
	Información del firmante(s) del documento (persona física, jurídica o sello de órgano).	Propiedades o etiquetas de la firma.
	Emisor del certificado del firmante(s).	Propiedades o etiquetas de la firma.
	Fecha y hora de la firma(s).	Propiedades o etiquetas de la firma.

§ 29

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13168

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Digitalización de Documentos establece los componentes de un documento electrónico digitalizado, incluyendo la imagen

electrónica, firma electrónica y metadatos, así como las reglas para la digitalización de documentos en soporte papel por parte de las Administraciones públicas, atendiendo a los formatos, niveles de calidad, condiciones técnicas y estándares aplicables; y para los aspectos relativos a la gestión y conservación de los documentos electrónicos digitalizados se remite a la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la Disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Digitalización de Documentos, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Digitalización de Documentos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE DIGITALIZACIÓN DE DOCUMENTOS

I. Objeto

La Norma Técnica de Interoperabilidad de Digitalización de Documentos tiene por objeto establecer los requisitos a cumplir en la digitalización de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización a través de medios fotoeléctricos.

II. Ámbito de aplicación

Esta norma será de aplicación en la digitalización de documentos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

III. Documentos electrónicos digitalizados

III.1 La digitalización de un documento para la generación de un documento electrónico atenderá a lo dispuesto en la Norma Técnica de Interoperabilidad de Documento Electrónico y estará compuesto por:

a) La imagen electrónica que representará el aspecto y contenido del documento en el soporte origen y cumplirá los requisitos establecidos en el apartado IV de esta norma.

b) Los metadatos mínimos obligatorios definidos en la Norma Técnica de Interoperabilidad de Documento Electrónico.

Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas del proceso de digitalización que se aplicarán, en su caso, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

c) Si procede, firma de la imagen electrónica de acuerdo con la normativa aplicable.

III.2 Para que el documento electrónico digitalizado sea copia auténtica del documento origen, se cumplirán, adicionalmente, los requisitos establecidos en la Norma Técnica de

Interoperabilidad de Procedimientos de Copiado Auténtico y Conversión entre Documentos Electrónicos.

IV. Requisitos de la imagen electrónica

IV.1 Las imágenes electrónicas aplicarán los formatos establecidos para ficheros de imagen en la Norma Técnica de Interoperabilidad de Catálogo de Estándares.

IV.2 El nivel de resolución mínimo para imágenes electrónicas será de 200 píxeles por pulgada, tanto para imágenes obtenidas en blanco y negro, color o escala de grises.

IV.3 La imagen electrónica será fiel al documento origen, para lo cual:

a) Respetará la geometría del documento origen en tamaños y proporciones.

b) No contendrá caracteres o gráficos que no figurasen en el documento origen.

c) Su generación atenderá a lo establecido en el apartado V de esta norma.

V. Proceso de digitalización

Con el fin de satisfacer los requisitos establecidos en el apartado IV, la digitalización de un documento:

1. Se realizará a través de un proceso informático en el que, garantizando la integridad de cada uno de los pasos, se realizarán las siguientes tareas:

a) Digitalización por un medio fotoeléctrico, de modo que se obtenga una imagen electrónica en la memoria del sistema asociado al dispositivo.

b) Si procede, optimización automática de la imagen electrónica para garantizar su legibilidad, de modo que todo contenido del documento origen pueda apreciarse y sea válido para su gestión (umbralización, reorientación, eliminación de bordes negros, u otros de naturaleza análoga).

c) Asignación de los metadatos al documento electrónico digitalizado según lo dispuesto en el apartado 111.1.

d) Si procede, firma de la imagen electrónica.

2. Contemplará la aplicación de un conjunto de operaciones de mantenimiento preventivo y comprobaciones rutinarias que permitirán garantizar mediante su cumplimiento que, en todo momento, el estado de la aplicación de digitalización y los dispositivos asociados producirán imágenes fieles al documento en soporte papel.

§ 30

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Expediente Electrónico

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13170

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Expediente electrónico establece la estructura de los expedientes electrónicos, que incluye documentos electrónicos, índice

electrónico, firma electrónica y metadatos mínimos obligatorios, así como las especificaciones para los servicios de remisión y puesta a disposición; para los aspectos relativos a la gestión y conservación de los expedientes electrónicos se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos; finalmente, se incluye en anexo la definición detallada de los metadatos mínimos obligatorios y los esquemas XML para el intercambio de expedientes electrónicos. En este sentido, la estructura de expediente electrónico definida en esta norma permite la utilización de las firmas electrónicas contempladas en la Decisión de la Comisión 2011/130/EU, de 25 de febrero de 2011, por la que se establecen los requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes en virtud de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Expediente electrónico, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Expediente electrónico que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE EXPEDIENTE ELECTRÓNICO

I. Objeto.

La Norma Técnica de Interoperabilidad de Expediente electrónico tiene por objeto establecer la estructura y el formato del expediente electrónico, así como las especificaciones de los servicios de remisión y puesta a disposición.

II. Ámbito de aplicación.

II.1 Esta norma será de aplicación a los expedientes electrónicos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

II.2 Las condiciones establecidas en esta norma se podrán aplicar a otros conjuntos de documentos electrónicos que, habiendo sido creados al margen de un procedimiento reglado, se hubiesen formado mediante agregación, como resultado de una secuencia de actuaciones coherentes que conducen a un resultado específico.

III. Componentes del expediente electrónico.

III.1 Los componentes de un expediente electrónico son:

a) Documentos electrónicos, que cumplirán las características de estructura y formato establecidas en la Norma Técnica de Interoperabilidad de Documento electrónico.

Los documentos electrónicos podrán incluirse en un expediente electrónico bien directamente como elementos independientes, bien dentro de una carpeta, entendida ésta como una agrupación de documentos electrónicos creada por un motivo funcional, o bien como parte de otro expediente, anidado en el primero.

b) Índice electrónico, que según lo establecido en el artículo 32.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, garantizará la integridad del expediente electrónico y permitirá su recuperación siempre que sea preciso.

El índice electrónico recogerá el conjunto de documentos electrónicos asociados al expediente en un momento dado y, si es el caso, su disposición en carpetas o expedientes.

c) Firma del índice electrónico por la Administración, órgano o entidad actuante de acuerdo con la normativa aplicable.

d) Metadatos del expediente electrónico.

III.2 La incorporación de un expediente electrónico a un sistema de gestión documental atenderá a lo dispuesto en la Norma Técnica de Interoperabilidad de Documento electrónico y en la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

IV. Metadatos del expediente electrónico.

IV.1 Los metadatos mínimos obligatorios del expediente electrónico:

a) Serán los definidos en el anexo I.

b) Se asociarán en la formación del expediente para su remisión o puesta a disposición.

c) No serán modificados en ninguna fase posterior del procedimiento administrativo, a excepción de modificaciones necesarias para la corrección de errores u omisiones en el valor inicialmente asignado.

IV.2 Se podrán asignar metadatos complementarios para atender a necesidades de descripción específicas. Estos metadatos complementarios se aplicarán, en su caso, de acuerdo con lo previsto en la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

V. Intercambio de expedientes electrónicos.

V.1 El intercambio de expedientes electrónicos, a los efectos de remisión y puesta a disposición, se realizará mediante el envío en primer lugar de la estructura definida en el anexo II, sin perjuicio de la aplicación de otras, reguladas por su normativa específica. Tras el envío de dicha estructura, se enviarán cada uno de los documentos electrónicos que componen el expediente, en el orden indicado en el índice y atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico.

V.2 Excepcionalmente, se podrán aplicar otras estructuras para el intercambio de expedientes electrónicos entre Administraciones públicas, cuando exista acuerdo previo entre las partes. En cualquier caso, si debe enviarse a un tercero, la estructura utilizada será convertida por el emisor a la estructura definida en el anexo II.

V.3 Cuando la naturaleza o la extensión de las pruebas o documentos que forman parte del expediente electrónico no permitan o dificulten notablemente su inclusión en una de las estructuras establecidas, se incorporará al expediente electrónico un documento en el que se especifique cuales son estas pruebas o documentos. Dichas pruebas o documentos serán custodiados por el órgano gestor sin perjuicio, en su caso, de aportación separada cuando así se requiera.

V.4 El índice electrónico de los expedientes objeto de intercambio reflejará, al menos:

a) La fecha de generación del índice.

b) Para cada documento electrónico: su identificador, su huella digital, la función resumen utilizada para su obtención, que atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares, y, opcionalmente, la fecha de incorporación al expediente y el orden del documento dentro del expediente.

c) Si es el caso, la disposición de los documentos en carpetas y expedientes electrónicos anidados.

V.5 Para el intercambio de expedientes electrónicos, entre Administraciones públicas, en procesos de actuación automatizada:

a) Se utilizará preferentemente la Red de comunicaciones de las Administraciones públicas españolas como medio para la transmisión.

b) Si el expediente electrónico forma parte de un asiento registral, éste será tratado como adjunto del mensaje de datos de intercambio según lo establecido en la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales.

V.6 En caso de intercambio de expedientes electrónicos entre Administraciones públicas que suponga una transferencia de custodia o traspaso de responsabilidad de gestión de expedientes que deban conservarse permanentemente, el órgano o entidad transferidora verificará la autenticidad e integridad del expediente en el momento de dicho intercambio.

ANEXOS

ANEXO I

Metadatos mínimos obligatorios de expedientes electrónicos

Metadato	Descripción/Condiciones de uso	¿Repetible?1 F[1]	Tipo	Esquema de valores
Versión NTI	Identificador normalizado de la versión de la Norma Técnica de Interoperabilidad de Expediente electrónico conforme a la cual se estructura el expediente.	1	URI	http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e
Identificador	Identificador normalizado del expediente.	1	Cadena de caracteres	ES <órganoUU><AAAA> EXP <ID especifico>2F[2] Ejemplo: ES_E00010207_2010_EXP_ MPR000000000000000000000010207
Órgano	Identificador normalizado de la administración responsable de la tramitación del procedimiento	1:N	Cadena de caracteres	Código alfanumérico único para cada órgano/unidad/oficina extraído del Directorio Común gestionado por el Ministerio de Política Territorial y Administración Pública. UEjemploU: E00003901
Fecha Apertura Expediente	Fecha de apertura del expediente	1	Fecha/hora	Formato: AAAAMMDD T HH:MM:SS <ISO 8601>
Clasificación	Procedimiento administrativo con el que se relaciona el expediente	1	Cadena de caracteres	Esquema de valores normalizado según el Sistema de Información Administrativa (SIA). Si el procedimiento no se encuentra en SIA: <órgano >_PRO_<ID_PRO_especifico>3F[3]
Estado	Estado del expediente en el momento de intercambio.	1	Cadena de caracteres	– Abierto – Cerrado – Índice para remisión cerrado.
Interesado	Identificador del interesado.	0:N	Cadena de caracteres	a) Si ciudadano o persona jurídica: DNI, NIE, NIF o similar. b) Si administración: <ÓrganoUU>
Tipo de firma	Indica el tipo de firma del índice del expediente	1:N	Cadena de caracteres	– CSV' – Formatos de firma electrónica de documentos electrónicos definidos en la Norma Técnica de Interoperabilidad de Política de firma y certificados de la Administración.
Si "Tipo de firma" = CSV				
Valor CSV	Valor del CSV.	1:N	Cadena de caracteres	N/A
Definición generación CSV	Referencia a la Orden, Resolución o documento que define la creación del CSV correspondiente.	1:N	Cadena de caracteres	Si AGE: Referencia BOE:BOE-A-YYYY-XXXXX En otro caso, referencia correspondiente.

[1] Nótese que la repetibilidad indicada en la tabla sólo se refiere a los metadatos que acompañan al expediente electrónico en un intercambio, sin perjuicio de la posibilidad de asignación de otros metadatos gestionados a nivel interno de cada administración cuyas consideraciones atenderán a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

[2] Codificación del Identificador del expediente:

<Órgano>: Véase codificación del metadato "Órgano". En caso de más de un órgano los nueve caracteres correspondientes serán acordados entre las partes con el fin de asegurar la unicidad del identificador que es su único fin.

<AAAA>: Año de la fecha de creación del expediente. (Longitud: 4 caracteres).

<ID_específico>: Código alfanumérico que identifica de forma única al expediente dentro de los generados por la administración responsable. Cada administración puede diseñar el proceso de generación según sus necesidades, asegurando en cualquier caso su unicidad. Por lo tanto, este ID puede generarse de forma secuencial o bien, ser una réplica del ID utilizado a nivel interno de la administración. (Longitud: 30 caracteres).

[3] Codificación del metadato Calificación si el procedimiento no existe en SIA:

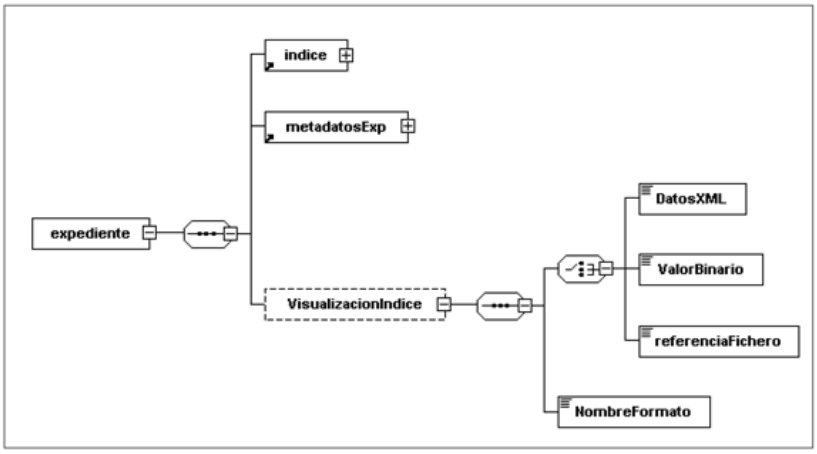
<Órgano>: Véase codificación del metadato "Órgano".

<ID_PRO_específico>: Código alfanumérico que identifica de forma única al procedimiento dentro de los propios de la administración. Cada administración puede diseñar el proceso de generación según susnecesidades, asegurando en cualquier caso su unicidad. Por lo tanto, este ID puede generarse de forma secuencial o bien, ser una réplica del ID utilizado a nivel interno de la administración. (Longitud: 30 caracteres).

ANEXO II

Esquemas XML para intercambio de expedientes electrónicos

1. *XSD Expediente electrónico*

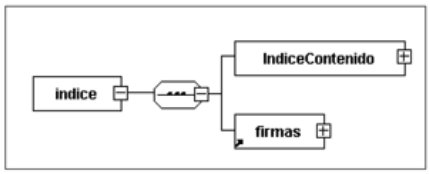



```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:eniexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e"
xmlns:eniexpmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos"
xmlns:eniexp="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD EXPEDIENTE ELECTRONICO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-
e/IndiceExpedienteEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-
e/metadatos/MetadatosExpedienteEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-
e/contenido/contenidoDocumentoEni.xsd"/>
<xsd:element name="expediente" type="eniexp:TipoExpediente"/>
<xsd:complexType name="TipoExpediente">
    <xsd:annotation>
        <xsd:documentation>
```

Para el intercambio de un expediente electrónico, se envía en primer lugar, el índice del expediente. Posteriormente, se enviarán los documentos que lo componen, uno a uno, y siguiendo la distribución reflejada en el contenido del Índice.

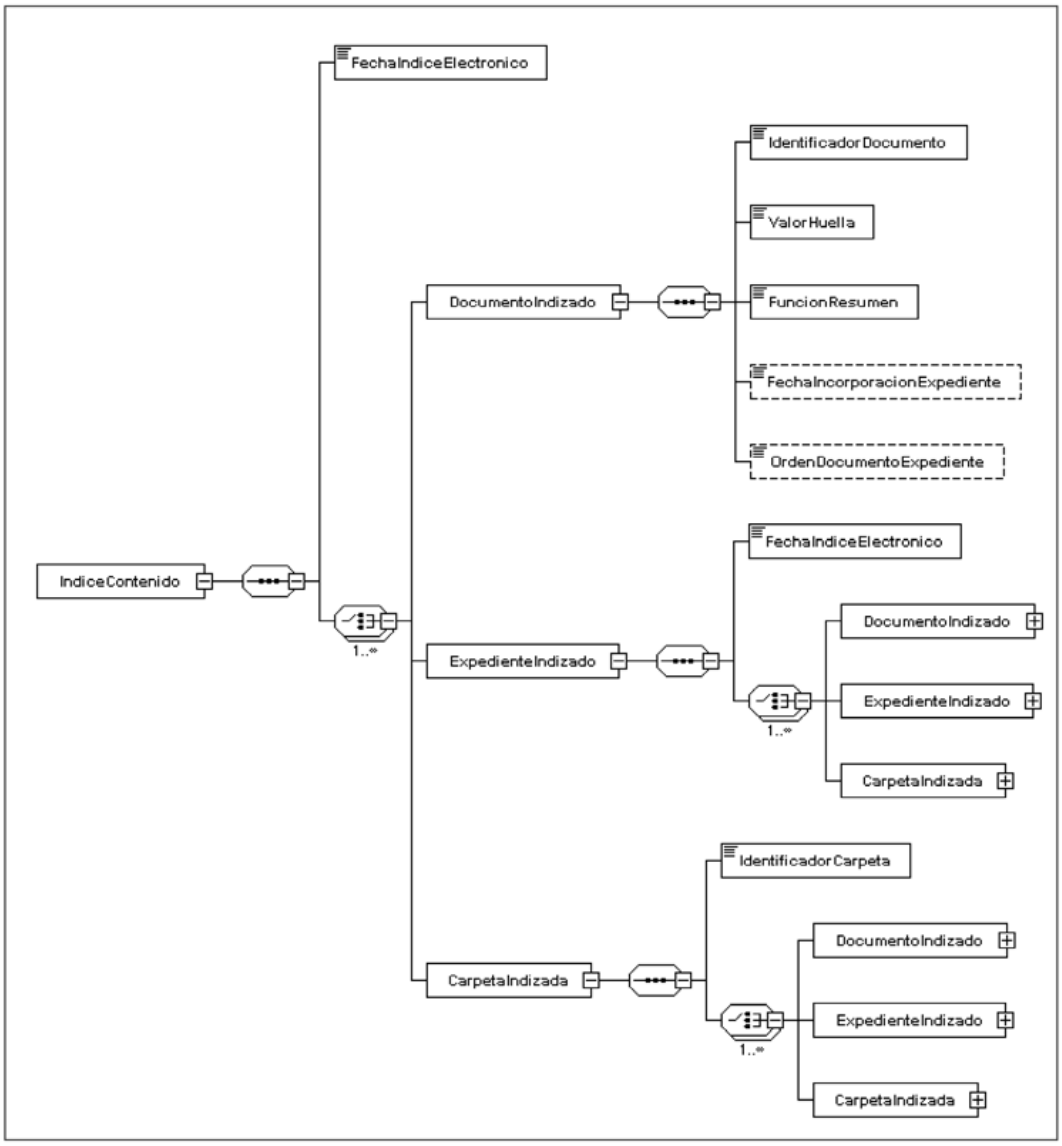
```
</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
        <xsd:element ref="eniexpind:indice"/>
        <xsd:element ref="eniexpmeta:metadatosExp"/>
        <xsd:element name="VisualizacionIndice" type="enifile:TipoContenido" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

2. *XSD Índice electrónico del expediente*



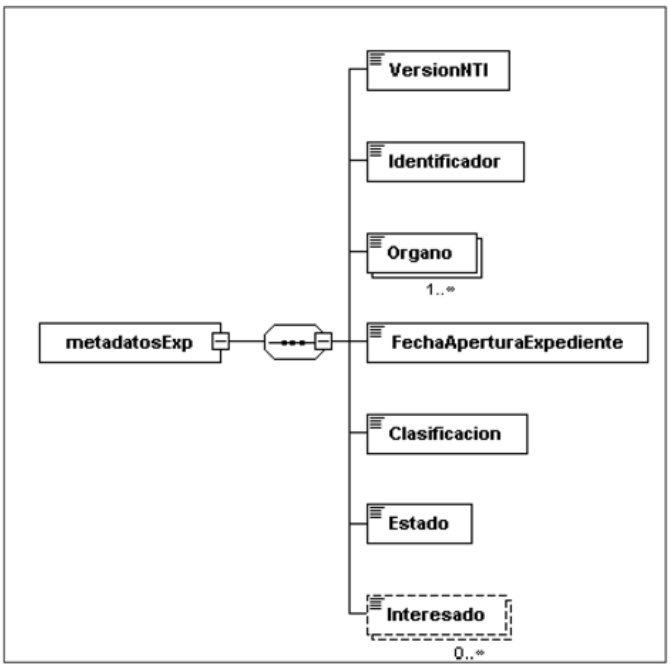

```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:eniexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e"
xmlns:eniconexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido" targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
<xsd:documentation xml:lang="es">XSD INDICE EXPEDIENTE ELECTRONICO ENI (v1.0)
</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma" schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma/firmasEni.xsd"/>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido"
schemaLocation="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-
e/contenido/IndiceContenidoExpedienteEni.xsd"/>
<xsd:element name="indice" type="eniexpind:TipoIndice"/>
<xsd:complexType name="TipoIndice">
    <xsd:sequence>
        <xsd:element name="IndiceContenido" type="eniconexpind:TipoIndiceContenido"/>
        <xsd:element ref="enids:firmas">
            <xsd:annotation>
<xsd:documentation>Existirá, al menos, una firma del contenido del índice del expediente electrónico.</xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

3. *XSD Contenido del índice electrónico del expediente*



```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:eniconexpind="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/indice-e/contenido" elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD CONTENIDO INDICE EXPEDIENTE ELECTRONICO ENI (v1.0) </xsd:documentation>
</xsd:annotation>
<xsd:element name="IndiceContenido" type="eniconexpind:TipoIndiceContenido"/>
<xsd:complexType name="TipoIndiceContenido">
    <xsd:sequence>
        <xsd:element name="FechaIndiceElectronico" type="xsd:dateTime"/>
        <xsd:choice maxOccurs="unbounded">
            <xsd:element name="DocumentoIndizado"
             type="eniconexpind:TipoDocumentoIndizado"/>
            <xsd:element name="ExpedienteIndizado"
             type="eniconexpind:TipoIndiceContenido"/>
            <xsd:element name="CarpetaIndizada" type="eniconexpind:TipoCarpetaIndizada"/>
        </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
<xsd:complexType name="TipoDocumentoIndizado">
    <xsd:sequence>
        <xsd:element name="IdentificadorDocumento" type="xsd:string"/>
        <xsd:element name="ValorHuella" type="xsd:string"/>
        <xsd:element name="FuncionResumen" type="xsd:string"/>
        <xsd:element name="FechaIncorporacionExpediente" type="xsd:dateTime" minOccurs="0"/>
        <xsd:element name="OrdenDocumentoExpediente" type="xsd:string" minOccurs="0"/>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
<xsd:complexType name="TipoCarpetaIndizada">
    <xsd:sequence>
        <xsd:element name="IdentificadorCarpeta" type="xsd:string"/>
        <xsd:choice maxOccurs="unbounded">
            <xsd:element name="DocumentoIndizado"
             type="eniconexpind:TipoDocumentoIndizado"/>
            <xsd:element name="ExpedienteIndizado"
             type="eniconexpind:TipoIndiceContenido"/>
            <xsd:element name="CarpetaIndizada" type="eniconexpind:TipoCarpetaIndizada"/>
        </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

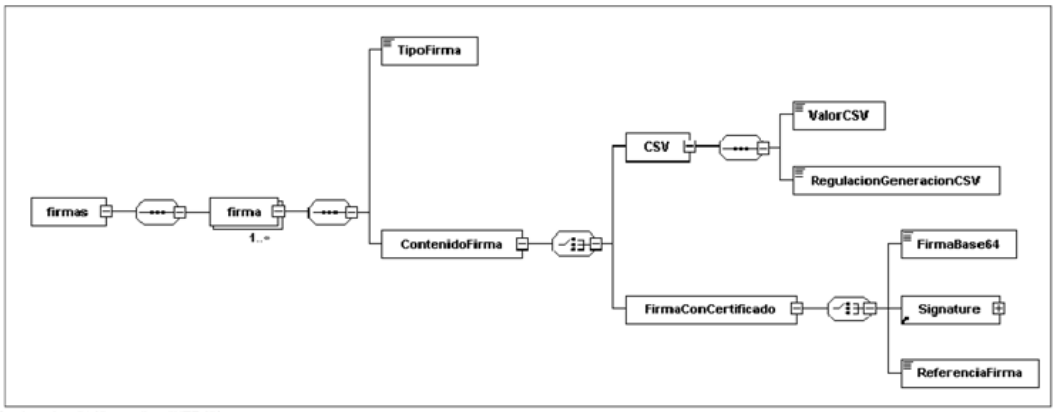
4. *XSD Metadatos del expediente electrónico*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:eniexpmeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/expediente-e/metadatos"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
<xsd:documentation xml:lang="es">XSD METADATOS EXPEDIENTE ELECTRONICO ENI (v1.0) </xsd:documentation>
</xsd:annotation>
<xsd:element name="metadatosExp" type="eniexpmeta:TipoMetadatos"/>
<xsd:complexType name="TipoMetadatos">
    <xsd:sequence>
        <xsd:element name="VersionNTI" type="xsd:anyURI"/>
        <xsd:element name="Identificador" type="xsd:string"/>
        <xsd:element name="Organo" type="xsd:string" minOccurs="1" maxOccurs="unbounded"/>
        <xsd:element name="FechaAperturaExpediente" type="xsd:dateTime"/>
        <xsd:element name="Clasificacion" type="xsd:string"/>
        <xsd:element name="Estado">
```

```
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
                - E01 - Abierto.
                - E02 - Cerrado.
                - E03 - Índice para remisión cerrado.
                </xsd:documentation>
            </xsd:annotation>
            <xsd:complexType>
                <xsd:simpleContent>
                    <xsd:extension base="eniexpmeta:enumeracionEstados"/>
                </xsd:simpleContent>
            </xsd:complexType>
        </xsd:element>
        <xsd:element name="Interesado" type="xsd:string" minOccurs="0" maxOccurs="unbounded">
            <xsd:annotation>
<xsd:documentation xml:lang="es">Obligatorio cumplimentar en caso de que exista al menos un interesado.</xsd:documentation>
            </xsd:annotation>
        </xsd:element>
    </xsd:sequence>
    <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>

<!-- Enumeración de Estados del expediente -->
<xsd:simpleType name="enumeracionEstados">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="E01"/>
        <xsd:enumeration value="E02"/>
        <xsd:enumeration value="E03"/>
    </xsd:restriction>
</xsd:simpleType>
</xsd:schema>
```

5. *XSD Firmas*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma "
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD FIRMAS ELECTRONICAS ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
 schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-schema.xsd"/>
<xsd:element name="firmas" type="enids:firmas"/>
<xsd:complexType name="firmas">
    <xsd:sequence>
        <xsd:element name="firma" type="enids:TipoFirmasElectronicas" minOccurs="1" maxOccurs="unbounded"/>
    </xsd:sequence>
</xsd:complexType>
<xsd:complexType name="TipoFirmasElectronicas">
    <xsd:sequence>
        <xsd:element name="TipoFirma">
            <xsd:annotation>
                <xsd:documentation xml:lang="es">
                    - TF01 - CSV.
                    - TF02 - XAdES internally detached signature.
                    - TF03 - XAdES enveloped signature.
                    - TF04 - CAdES detached/explicit signature.
                    - TF05 - CAdES attached/implicit signature.
```

```
                - TF06 - PAdES.
            </xsd:documentation>
        </xsd:annotation>
        <xsd:simpleType>
            <xsd:restriction base="xsd:string">
                <xsd:enumeration value="TF01"/>
                <xsd:enumeration value="TF02"/>
                <xsd:enumeration value="TF03"/>
                <xsd:enumeration value="TF04"/>
                <xsd:enumeration value="TF05"/>
                <xsd:enumeration value="TF06"/>
            </xsd:restriction>
        </xsd:simpleType>
    </xsd:element>
    <xsd:element name="ContenidoFirma">
        <xsd:complexType>
            <xsd:choice>
                <xsd:element name="CSV">
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="ValorCSV" type="xsd:string"/>
                            <xsd:element name="RegulacionGeneracionCSV" type="xsd:string"/>
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="FirmaConCertificado">
                    <xsd:complexType>
                        <xsd:choice>
                            <xsd:element name="FirmaBase64" type="xsd:base64Binary"/>
                            <xsd:element ref="ds:Signature"/>
                            <xsd:element name="ReferenciaFirma">
                                <xsd:annotation>
                                <xsd:documentation  xml:lang="es"> Referencia interna al fichero que incluye la firma. </xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                        </xsd:choice>
                    </xsd:complexType>
                </xsd:element>
            </xsd:choice>
        </xsd:complexType>
    </xsd:element>
</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
<xsd:attribute name="ref" type="xsd:string" use="optional">
    <xsd:annotation>
        <xsd:documentation xml:lang="es">Almacena el identificador del nodo que se está firmando. En caso de firmas multinodo, se incluirá una lista separada por comas de los identificadores
        de los nodos firmados. </xsd:documentation>
    </xsd:annotation>
</xsd:attribute>
</xsd:complexType>
</xsd:schema>
```

§ 31

Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 266, de 3 de noviembre de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-10146

El Esquema Nacional de Interoperabilidad se establece en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, en el marco, entre otras normas, de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma y sello, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y reutilización de la información del sector público; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, según se establece en el artículo 29 del Esquema Nacional de Interoperabilidad.

En particular, la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración se aprobó mediante Resolución de 19 de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, para responder a lo previsto en el artículo 18 del citado Real Decreto 4/2010, de 8 de enero, sobre la interoperabilidad en materia de firma y sello electrónicos y de certificados.

Posteriormente, la evolución de las tecnologías de aplicación, la experiencia derivada de la aplicación de la citada Norma Técnica de Interoperabilidad, la entrada en vigor de la citada Ley 40/2015, de 1 de octubre, y la evolución del contexto regulatorio europeo, particularmente por razón del Reglamento n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y su normativa de desarrollo, hacen necesario una actualización de esta Norma Técnica de Interoperabilidad.

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye a la anterior denominada de Política de Firma Electrónica y de certificados de la Administración, establece el conjunto de criterios para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de las Administraciones públicas. Para ello, define el contenido de una política de firma electrónica y sello electrónico basados en certificados, especificando las características de las reglas comunes, como formatos, uso de algoritmos, creación y validación de firma para documentos electrónicos, así como de las reglas de confianza en certificados electrónicos, sellos de tiempo y firmas longevas.

Las condiciones establecidas en esta norma persiguen establecer un marco para la definición de políticas de firma y sello electrónicos basada en certificados alineada con actos europeos recientes como la Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, compatible a su vez con sistemas de firma electrónica ya implantados.

La presente actualización de la norma técnica se ha elaborado con la participación de todas las Administraciones Públicas a las que les es de aplicación, ha sido informada favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración, que sustituye completamente a la anterior Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, y cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la Administración que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

NORMA TÉCNICA DE INTEROPERABILIDAD DE POLÍTICA DE FIRMA Y SELLO ELECTRÓNICOS Y DE CERTIFICADOS DE LA ADMINISTRACIÓN

I Consideraciones generales

I.1 Objeto.

1. La Norma Técnica de Interoperabilidad (en adelante, NTI) de Política de firma y sello electrónicos y de certificados de la Administración tiene por objeto establecer el conjunto de criterios comunes asumidos por la Administración pública en relación con la autenticación y el reconocimiento mutuo de firmas electrónicas y sellos electrónicos basados en certificados

electrónicos cualificados o reconocidos y que, como tales, serán desarrollados y consolidados a través de las políticas de firma y sello electrónicos basados en certificados.

2. El objetivo final de esta NTI es facilitar el uso de firmas electrónicas y sellos electrónicos seguros e interoperables entre las distintas organizaciones de la Administración pública.

I.2 Ámbito de aplicación.

1. El contenido de esta NTI será de aplicación para el desarrollo o adopción de políticas de firma y sello electrónicos basada en certificados por parte de cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organizaciones) según el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. Las políticas de firma y sello harán referencia a un contexto concreto de carácter horizontal donde sea necesario normalizar aspectos de las firmas electrónicas de los Documentos Electrónicos Administrativos para garantizar la interoperabilidad, no a una Administración u organismo particular. Para establecer los aspectos técnicos de las firmas dentro de una Administración u organismos concreto, se optará por la generación de instrucciones técnicas internas, procedimientos o directrices de aplicaciones, que en todo caso deberán ajustarse a lo establecido por el Esquema Nacional de Seguridad.

II La política de firma y sello electrónicos

II.1 Definición y contenido.

1. Según la definición del Real Decreto 4/2010, de 8 de enero, una política de firma electrónica es el «conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma». Es de aplicación tanto a las firmas como a los sellos electrónicos.

2. Una política de firma y sello electrónicos y de certificados definirá:

a) Los procesos de creación, validación y conservación de firmas electrónicas y sellos electrónicos.

b) Características y requisitos de los sistemas de firma electrónica, sellos electrónicos, certificados y sellos de tiempo.

3. Toda política de firma y sello electrónicos basada en certificados incluirá:

a) Definición del alcance y ámbito de aplicación, que concretará su relación con otras políticas existentes, marco o particulares, así como la identificación de los actores involucrados y los usos de la firma electrónica y sello electrónico.

b) Datos para la identificación del documento y del responsable de su gestión.

c) Reglas comunes para el firmante, el creador del sello, y el verificador de la firma o sello electrónicos que incluirán:

i. Formatos admitidos de firma electrónica y sello electrónico, y reglas de uso de algoritmos.

ii. Reglas de creación de firma o sello electrónicos.

iii. Reglas de validación de firma o sello electrónicos.

d) Reglas de confianza, que incluirán los requisitos establecidos para certificados, sellos de tiempo y firmas longevas.

e) Otras reglas opcionales a fijar por cada organización, como podrán ser:

i. Reglas específicas de compromisos que cada organización podrá establecer para cada uno de los servicios que presta, estableciendo requisitos específicos necesarios para que la firma sea válida en cada caso.

ii. Reglas de certificados de atributos mediante las que cada organización podrá establecer información adicional a añadir a los certificados digitales en función de sus necesidades y del contexto.

f) Definición de condiciones para el archivado y custodia de firmas electrónicas.
g) Descripción de consideraciones de gestión de la política que se aplicarán a dicho documento.

II.2 Datos identificativos de la política.

1. El documento de política de firma y sello incluirá la siguiente información para su identificación:

a) Nombre del documento.
b) Versión.
c) Identificador (OID Object IDentifier) de la política.
d) URI (Uniform Resource Identifier) de referencia de la política.
e) Fecha de expedición.
f) Ámbito de aplicación.

2. La política de firma y sello incluirá la definición de su periodo de validez y las consideraciones respecto a los periodos de transición que procedan.
3. Para la identificación de su gestor, la política de firma y sello electrónicos basada en certificados incluirá:

a) Nombre del gestor de la política.
b) Dirección de contacto.
c) OID del gestor de la política de firma.

II.3 Actores involucrados en la firma electrónica.

Los actores involucrados en el proceso de creación y validación de una firma electrónica serán:

a) Firmante: Una persona física que crea una firma electrónica utilizando datos de creación de firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa.
b) Creador de un sello: Una persona jurídica que crea un sello electrónico.
c) Verificador: Entidad, ya sea persona física o jurídica, que valida o verifica una firma electrónica apoyándose en las condiciones exigidas por la política de firma y sello concreta por la que se rige la plataforma de relación electrónica o el servicio concreto al que se esté invocando. Podrá ser una entidad de validación de confianza o una tercera parte que esté interesada en la validez de una firma electrónica.
d) Prestador de servicios de confianza (PSC): Una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianza.
e) Emisor y gestor de la política de firma: Entidad que se encarga de generar y gestionar el documento de política de firma y sello, por el cual se deben regir el firmante, el verificador y los prestadores de servicios en los procesos de generación y validación de firma electrónica.

En este documento que utilizará el término ‘firmante’, tanto para referirse al firmante como al creador de un sello. Puede tratarse de un proceso de actuación administrativa automatizada.
Se usará el término ‘firma’ tanto para referirse a la firma electrónica como a sello electrónico.

II.4 Usos de la firma electrónica.

Las políticas de firma y sello electrónicos podrán definir condiciones para la aplicación de una firma electrónica basada en certificados con los siguientes propósitos:

a) Firma de transmisiones de datos, como herramienta para proporcionar seguridad al intercambio, garantizando la autenticación de los actores involucrados en el proceso, la integridad del contenido del mensaje de datos enviado y el no repudio de los mensajes en una comunicación telemática.

b) Firma de contenido como herramienta para garantizar la autenticidad, integridad y no repudio de aquel, con independencia de que forme parte de una transmisión de datos.

II.5 Interacción con otras políticas.

1. Las Administraciones Públicas se acogerán preferentemente a la Política Marco de Firma Electrónica basada en Certificados

a. Cada organización valorará la necesidad y conveniencia de desarrollar una política propia frente a la posibilidad de utilizar una política marco existente.
b. Las Administraciones Públicas podrán aprobar otras políticas de firma y sello electrónicos dentro de sus ámbitos competenciales si las características particulares de los procedimientos administrativos bajo su competencia lo hacen necesario. Las políticas de firma y sello particulares estarán orientadas a un contexto concreto, de carácter horizontal, no a una organización concreta. En el caso de que en una organización se deseen normalizar únicamente aspectos técnicos de las firmas electrónicas, se optará por otro instrumento distinto de una Política de firma y sello, como instrucciones técnicas internas o directrices de aplicaciones.
c. Serán aprobadas con informe favorable del Comité Sectorial de Administración Electrónica y del Comité Ejecutivo de la Comisión de Estrategia TIC, una vez verificada su interoperabilidad con la Política Marco de Firma Electrónica basada en Certificados.
d. Con objeto de permitir la interoperabilidad de las firmas electrónicas acordes a políticas, las políticas que las Administraciones Públicas aprueben deberán ser comunicadas, junto con sus correspondientes ficheros de implementación, a la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.

2. La definición del alcance y ámbito de aplicación de una política de firma y sello electrónicos se realizará considerando su interacción con otras políticas de firma y sello electrónicos, y asegurando que:

a) Su desarrollo es interoperable con la política marco, en caso de políticas de firma y sello particulares.
b) Define las condiciones de utilización y convivencia con otras políticas particulares, si se trata de una política marco.

3. En toda política de firma y sello electrónicos se asegurará que:

a) Las extensiones o restricciones establecidas para las reglas de creación o validación de firma atienden a la validación de los formatos de firma establecidos en esta NTI y política marco si procede, de forma que se garantice la interoperabilidad entre las diferentes organizaciones.
b) Incluye, si procede, la referencia a la URL de la política marco de firma electrónica en la que se inscribe, con indicación expresa de la versión.
c) Las firmas que se generen siguiendo políticas marco o particulares, incluyen un campo donde se indique de forma explícita la política a la que pertenecen.
d) Para que otras aplicaciones puedan interpretar las reglas de una política particular correctamente, dicha política está disponible en formato XML (eXtensible Markup Language) y ASN.1 (Abstract Syntax Notation One).

II.6 Gestión de la política de firma y sello.

1. La política de firma y sello electrónicos incluirá la descripción básica de su proceso de gestión, estableciendo las directrices para su mantenimiento, actualización y publicación, e identificando al responsable de llevar a cabo estas tareas.
2. El gestor de la política de firma mantendrá actualizada la versión de la política de firma y sello atendiendo a:

a) Modificaciones motivadas por necesidades propias de la organización.
b) Cambios en políticas relacionadas.
c) Cambios en los certificados electrónicos emitidos por los prestadores de servicios de certificación referenciados en la política de firma y sello.

3. Para facilitar la validación de firmas electrónicas creadas atendiendo a versiones anteriores de una política, se podrá mantener un repositorio con el historial de versiones anteriores que provea la ubicación de cada versión.

II.7 Archivado y custodia.

1. Atendiendo a las necesidades y normativa específicas de su ámbito, las políticas de firma y sello podrán contemplar la definición de condiciones y responsabilidades para el archivado y custodia de las firmas electrónicas en sus diferentes aplicaciones.

2. Para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se podrán utilizar:

a) Firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza, aplicando las reglas de confianza para firmas longevas descritas en el subapartado IV.3.

b) Otros métodos técnicos que impedirán la modificación de la firma para la que se ha verificado su validez, de acuerdo a los requisitos establecidos en la política de firma y sello correspondiente, y que habrá sido almacenada en un sistema en un momento del tiempo determinado. Todos los cambios que se realicen sobre el sistema en el que se encuentra almacenada la firma podrán auditarse para asegurar que dicha firma no ha sido modificada. Los requisitos de seguridad de dichos sistemas cumplirán con las condiciones de los niveles de seguridad establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Cada política de firma y sello definirá un servicio para mantener las evidencias de validez de las firmas longevas y gestionar la actualización de las firmas y sellos. Dicho servicio especificará los mecanismos y condiciones bajo los que se archiva y custodia tanto la propia firma o sello como los certificados e informaciones de estado utilizadas en su validación.

4. El almacenamiento de los certificados y las informaciones de estado podrá realizarse dentro del fichero resultante de la firma electrónica o en un depósito específico:

a) En caso de almacenar los certificados y las informaciones de estado dentro de la firma, se sellarán también dichas informaciones, siguiendo las modalidades de firmas recogidas en la «Decisión de Ejecución UE 2015/1506 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público», o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

b) Si los certificados y las informaciones de estado se almacenan en un depósito específico, se sellarán de forma independiente.

5. La protección de la firma/sello electrónico frente a la posible obsolescencia de los algoritmos y el aseguramiento de sus características a lo largo del tiempo de validez, se realizará a través de uno de los siguientes procesos:

a) Utilización de mecanismos de resellado de tiempo, para añadir, cuando el anterior sellado este próximo a su caducidad, un sello de fecha y hora de archivo con un algoritmo más robusto.

b) Se recomienda utilizar mecanismos de resellado/refirma, en el caso de obsolescencia de los algoritmos o formatos, con un algoritmo más robusto.

c) Almacenamiento de la firma electrónica en un depósito seguro, que garantice la protección de la firma contra modificaciones y asegurando la fecha exacta en que se guardó la firma electrónica, y en la que se comprobó la autenticidad y vigencia de los elementos que la conforman.

d) Otros sistemas que garanticen la preservación de las firmas y sellos a largo plazo con certeza de la comprobación de su validez en el momento más próximo que sea posible respecto a su generación o admisión. Estos sistemas adicionales deberán estar descritos

minuciosamente en el documento de gestión de política de custodia documental de la entidad, con indicación de los plazos en los que los sistemas estuvieron vigentes y los archivos a los que estos sistemas se aplicaron, especialmente para el caso de valoración documental a largo plazo por especialistas en archivos.

6. La definición de medidas y procedimientos para archivado y custodia de firmas/sellos electrónicos se realizará atendiendo con proporcionalidad a los diferentes usos de la firma electrónica contemplados en el alcance y ámbito de aplicación de la política.

7. Para archivado y gestión de documentos electrónicos firmados o sellados, se atenderá a lo establecido en la NTI de Política de gestión de documentos electrónicos.

III Reglas comunes

III.1 Reglas comunes.

1. Las reglas comunes permitirán establecer responsabilidades respecto a la firma/sello electrónicos sobre la persona o entidad que crea la firma y la persona o entidad que la verifica, definiendo los requisitos mínimos que deben presentarse, debiendo estar firmados si son requisitos para el firmante, o no firmados si son requisitos para el verificador.

2. Estas reglas se definirán en base a los formatos de firma/sello electrónico admitidos, teniendo en cuenta los diferentes usos de la firma electrónica basada en certificados, al uso de algoritmos y a los procesos de creación y validación de firma y sello.

III.2 Formatos admitidos de firma electrónica.

1. Los formatos admitidos por las organizaciones para las firmas/sellos electrónicos basadas en certificados electrónicos, se ajustarán a:

a) la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior».

b) lo establecido en la NTI de Catálogo de estándares.

c) los formatos CAdES, XAdES y PAdES en las versiones establecidas en la Norma Técnica de Interoperabilidad de Política de firma del 2011.

2. Los formatos de firma/sello electrónico serán

a) Si procede, interoperables con la política marco en la que se basan.

III.3 Formatos de firma electrónica de transmisiones de datos.

1. La firma electrónica de transmisiones de datos estará basada en estándares recogidos en la NTI de Catálogo de estándares, siendo responsabilidad del emisor y gestor de la política la definición de las consideraciones concretas a aplicar por cada organización.

2. Cada política definirá las versiones soportadas así como los cambios en aquellas que pueden provocar una actualización de dicha política.

III.4 Formatos de firma/sello electrónica de contenido.

1. Los formatos para la firma/sello electrónica de contenido se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014»

2. Por compatibilidad con las políticas de firma anteriores, se permitirán aunque no se recomiendan los siguientes formatos::

a) XAdES (XML Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 903, versión 1.2.2 y versión 1.3.2.

b) CAdES (CMS Advanced Electronic Signatures), según la especificación técnica ETSI TS 101 733, versión 1.6.3 y versión 1.7.4.

c) PAdES (PDF Advanced Electronic Signatures), según la especificación técnica ETSI TS 102 778-3.

3. El perfil mínimo de formato que se utilizará para la generación de firmas de contenido en el marco de una política será «-EPES», esto es, clase básica (BES) añadiendo

información sobre la política de firma y sello. En cualquier caso, cada organización podrá definir en su política de firma y sello las consideraciones adicionales que considere respecto a la interpretación y utilización de diferentes perfiles y clases de los formatos siempre en consonancia con lo establecido en esta NTI.

4. Las organizaciones aplicarán consideraciones de casos particulares para firma de contenido, al menos, en los siguientes casos:

a) Los documentos electrónicos a los que se aplique firma/sello basada en certificados de cara a su intercambio se ajustarán a las especificaciones de formato y estructura establecidas en la NTI de Documento electrónico.

El formato de firma basada en certificados que acompaña a un documento electrónico se reflejará en el metadato mínimo obligatorio definido en la NTI de Documento electrónico 'Tipo de firma', que, en este caso, podrá tomar uno de los siguientes valores:

i. XAdES internally detached signature.
ii. XAdES enveloped signature.
iii. CAdES detached/explicit signature.
iv. CAdES attached/implicit signature.
v. PAdES.
vi. XAdES (Decision 1506) detached
vii. XAdES (Decision 1506) enveloped
viii. CAdES (Decision 1506) detached
ix. CAdES (Decision 1506) attached
x. PAdES (Decision 1506)

b) La firma/sello de facturas electrónicas según el formato «Facturae» se realizará conforme a lo regulado por la Orden PRE/2971/2007, de 5 de octubre, o normativa que la sustituya.

III.5 Reglas de uso de algoritmos.

1. La política de firma y sello especificará las reglas de uso de algoritmos en los diferentes formatos así como la longitud de las claves asociadas a aquéllos de forma proporcional a las necesidades detectadas en los diferentes usos de la firma/sello electrónicos, cumpliendo en cualquier caso lo establecido en la NTI de Catálogo de estándares y lo previsto en las normas que se definan en aplicación del Reglamento (UE) 910/2014.

2. Para los entornos de seguridad regulados por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/ 2015, de 1 de octubre, de Régimen Jurídico del Sector Público, de aplicación en los procedimientos de administración electrónica, se ajustarán a la «Decisión de Ejecución UE 2015/1506» o en la que la sustituya, de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del «Reglamento (UE) 910/2014» o las especificaciones técnicas publicadas por los organismos de Estandarización Europeos. La definición de usos de algoritmos podrá contemplar diferentes posibilidades según lo establecido en las guías aplicables, como la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía, las normas ETSI TS 119 312 'Criptographic Suites for secure electronic signatures', o aquellas que las sustituyan.

3. Para los entornos de alta seguridad, de acuerdo con el criterio del Centro Criptológico Nacional (CCN) serán de aplicación las recomendaciones revisadas de la CCN-STIC 405 así como en la norma CCN-STIC 807 del Esquema Nacional de Seguridad relativa al uso de criptografía.

III.6 Reglas de creación de firma electrónica.

1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, se generará la firma electrónica.

2. Las plataformas que presten el servicio de creación de firma electrónica proporcionarán las funcionalidades necesarias para soportar un proceso de creación de firmas y sellos basado en los siguientes puntos:

a) Selección por parte del usuario firmante del fichero, formulario u otro objeto binario para ser firmado. Los formatos de ficheros atenderán a lo recogido en la NTI de Catálogo de estándares.

El firmante se asegurará de que el fichero que se quiere firmar no contiene contenido dinámico que afecte a su validez y que pudiese modificar el resultado de la firma/sello a lo largo del tiempo.

b) El servicio de firma electrónica ejecutará las siguientes verificaciones previas a la creación de la firma:

i. La firma/sello electrónicos pueden ser validados para el formato del fichero específico que va a ser firmado.

ii. Validez del certificado, comprobando si el certificado ha sido revocado, o suspendido, si entra dentro de su periodo de validez, y la validación de la cadena de certificación, incluyendo la validación de todos los certificados en la cadena, y de su vigencia y estado de no revocación, y si el certificado ha sido expedido por un Prestador de Servicios de Confianza Cualificado, incluido en la TSL del país emisor.

Si alguna de estas verificaciones es errónea, el proceso de firma se interrumpirá.

Si no fuese posible realizar estas comprobaciones en el momento de la firma, será necesario, en todo caso, que los sistemas receptores de la firma asuman dicha validación, antes de aceptar el fichero, formulario u otro objeto binario firmado.

c) El servicio creará un fichero con la firma/sello según corresponda en función del formato utilizado.

En el momento de la firma, se incluirá la referencia del identificador único de la versión del documento de política de firma y sello electrónicos en el que se ha basado su creación.

3. La vinculación del firmante se establecerá a través de etiquetas que, incluidas bajo la firma, y definidas según los estándares correspondientes (XAdES, CAdES y/o PAdES), proporcionarán la siguiente información complementaria a ésta:

a) Fecha y hora de firma, que podrá ser meramente indicativa en función de cómo se haya generado la firma.

b) Certificado del firmante.

c) Cadena de validación.

d) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica.

e) Formato del objeto original.

4. Como datos opcionales, la firma/sello electrónicos podrá incluir:

a) Lugar geográfico donde se ha realizado la firma del documento.

b) Rol de la persona firmante en la firma electrónica.

c) Acción del firmante sobre el documento firmado (lo aprueba, lo informa, lo recibe, lo certifica, etc.).

d) Sello de tiempo sobre algunos o todos los objetos de la firma.

5. En caso de creación de firmas/sellos electrónicos por distintos firmantes sobre un mismo objeto, donde el segundo firmante ratifica la firma del primero se utilizará la etiqueta correspondiente, CounterSignature, para contabilizarlas.

6. En el caso de que las múltiples firmas/sellos se realicen al mismo nivel, cada una de ellas se representará como una firma independiente.

III.7 Reglas de validación de firma/sello electrónicos.

1. Las políticas de firma y sello definirán las condiciones particulares bajo las que, en su ámbito, será posible validar la firma electrónica de un documentosiguiendo los requisitos establecidos en el artículo 32.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2. En el caso de documentos electrónicos, para acceder a la visualización de la firma/sello, el usuario podrá presentar dicho documento electrónico, que contenga los datos,

metadatos y firmas/sellos, en una sede electrónica o en otros sistemas generales que proporcionen herramientas de reproducción de documentos electrónicos.

3. Las condiciones mínimas que se producirán para la validación de la firma/sello serán las siguientes:

a) Garantía de que la firma es válida para el fichero específico que está firmado.

b) Validez de los certificados:

i. El instante de tiempo que se tomará como referencia para la validación será:

1) El momento en que se produjo la firma/sello si se da alguno de los siguientes supuestos:

a. los servicios de los prestadores facilitan los históricos de estado de los certificados y la firma/sello lleva un sello de tiempo válido en el momento de la verificación.

b. se trata de firmas/sellos longevos que incluyen las evidencias de la validez de la firma electrónica en el momento de la generación o primera validación, y dichas evidencias se encuentran selladas con un sello de tiempo válido.

2) En otros casos, el momento de la validación.

ii. Se comprobará que los certificados no fueron revocados ni suspendidos y que no han expirado.

iii. Se comprobará la validez de toda la cadena de certificación, incluyendo todos los certificados que la componen, con independencia de que éstos se encuentren incluidos en la propia firma o no.

iv. Se verificará que el certificado ha sido expedido por un prestador de servicios de certificación de confianza bajo una Declaración de Prácticas de Certificación que cumplirá la normativa y estará incluido en la política de firma y sello aplicable, y ha sido expedido por un Prestador de Servicios de Confianza Cualificado, incluido en la TSL del país emisor.

v. Verificación, si existen y si así lo requiere la política de la plataforma de relación electrónica o un servicio concreto de dicha plataforma, de los sellos de tiempo de los formatos implementados, incluyendo la verificación de los periodos de validez de los sellos de tiempo.

4. Para validar la firma electrónica se considerará la siguiente información:

a) Fecha y hora de la firma/sello: Si se ha realizado el sellado de tiempo, el sello de tiempo más antiguo dentro de la estructura de la firma se utilizará para determinar la fecha de la firma/sello. En caso de que no existan sellos de tiempo, la fecha y hora de la firma tendrán carácter indicativo, pero no se utilizarán para determinar el momento en que se realizó la firma. En caso de que no existan sellos de tiempo en la firma, la validación del certificado se realizará en el momento de la validación de la firma/sello.

b) Certificado del firmante. Este campo se utilizará para verificar el estado del certificado, y en su caso la cadena de certificación, en la fecha de la generación de la firma/sello.

c) Política de firma y sello sobre la que se basa el proceso de generación de firma electrónica. Se utilizará para identificar, mediante su hash y su identificador (OID), que la política de firma y sello que se ha utilizado para la generación de la firma se corresponde con la que se utilizará para el servicio en cuestión.

Esta validación de la política de firma y sello, implicará que el verificador dispondrá de los medios para verificar las condiciones impuestas en la política de firma y sello concreta. La disponibilidad de la política de firma y sello en un formato interpretable por medios automatizados (XML o ASN.1) y siguiendo los estándares europeos de representación de políticas de firma, indicada en el epígrafe 3.d del subapartado II.5 de esta NTI, facilitará la labor de las aplicaciones receptoras de firmas electrónicas en aplicar distintas políticas de firma y sello.

5. Si se han realizado varias firmas/sellos sobre un mismo documento, se seguirá el mismo proceso de verificación que con la primera firma/sello, comprobando cada firma o la etiqueta CounterSignature en el campo de propiedades no firmadas, donde se informa de los refrendos de firma generados.

6. El encargado de la verificación de la firma/sello podrá definir sus procesos de validación y de archivado, siempre en consonancia con los requisitos de la política de firma y

sello a la que se ajuste el servicio y con lo establecido en la NTI de Política de gestión de documentos electrónicos.

7. Para la verificación del estado de los certificados en el caso de formatos de firma longeva, la validez de la firma/sello vendrá determinada por la validez del sello de tiempo de las evidencias de la validación incluidas en la firma. En estos casos la validez de la firma/sello a lo largo del tiempo se mantendrá resellando la firma/sello antes de la caducidad del certificado de la TSA (Autoridad de sellado de tiempo) que realizó el sello de tiempo anterior, de forma que siempre sea posible verificar que en el momento en que se realizó la firma/sello, el certificado era válido.

8. En el caso de validación por un tercero, el validador ofrecerá a la parte usuaria el resultado correcto del proceso de validación.

IV Reglas de confianza

IV.1 Reglas de confianza para los certificados electrónicos.

1. Las políticas de firma y sello, marco o particulares, podrán fijar limitaciones y restricciones específicas para los certificados electrónicos que admiten en cada uno de los servicios que corresponda, si el uso destinado del certificado establecido en su Política de Certificación no está acorde al ámbito de la Política de firma y sello, siempre en consideración de la normativa aplicable en cada caso.

2. Se presumirán válidos los certificados cualificados que usen los ciudadanos en las firmas y sellos electrónicos. Si una administración apreciara algún aspecto que cuestionara esta validez lo hará saber al ciudadano que dispondrá del plazo previsto en la normativa de procedimiento administrativo para subsanar lo que corresponda o ratificar por otra vía los documentos firmados electrónicamente. El firmante no podrá alegar que ha utilizado una firma inválida con arreglo a una determinada Declaración de Prácticas de Certificación como condición en la que se base un recurso de nulidad o anulabilidad de un acto.

3. Los certificados válidos para ejecutar la firma/sello electrónicos de contenido serán los certificados electrónicos cualificados de firma y sello según el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

4. La relación de prestadores de servicios de certificación que emiten certificados electrónicos cualificados se consultará en la TSL (Lista de servicios de confianza) publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo y en las TSL del resto de países de la UE, de conformidad con la Decisión de Ejecución UE 2015/1505 de la Comisión, de 8 de septiembre de 2015, por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

5. La política de firma y sello electrónicos podrá establecer el período de precaución o de gracia que corresponda aplicar para la validación de los certificados. Este periodo podrá ser, desde el momento en que se realiza la firma o el sellado de tiempo, como mínimo, el tiempo máximo permitido para el refresco completo de las CRLs (Certificate Revocation Lists) o el tiempo máximo de actualización del estado del certificado en el servicio OCSP (Online Certificate Status Protocol). Esta definición tendrá en cuenta también la posibilidad de que estos tiempos varíen según el Prestador de Servicios de Certificación.

6. El verificador validará los certificados electrónicos en base a los procesos de validación y archivado definidos en la política de firma y sello a la que se ajuste el servicio en cada caso.

IV.2 Reglas de confianza para sellos de tiempo.

1. Los sellos cualificados de tiempo cumplirán los indicados en el artículo 42.1 del Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las

transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

2. Los elementos básicos de un sello cualificado de tiempo serán los indicados en las Normas Europeas de estandarización:

a) ETSI EN 319 422 V1.1.1Time-stamping protocol and time-stamp token profiles.

b) ETSI EN 319 421 V1.1.1 Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.

O en las que las sustituyan.

3. El sellado de tiempo y la información de validación podrán ser añadidos por el emisor, el receptor o un tercero y se incluirán como propiedades no firmadas en los campos correspondientes según el formato de firma utilizado.

4. En la política de firma y sello se establecerán las condiciones según las que determinar los sellos de tiempo admitidos atendiendo a sus necesidades particulares, y en base a la normativa y legislación vigente. Esto incluye el establecimiento del tiempo máximo aceptable para realizar el sellado de tiempo, anterior, en cualquier caso, a la caducidad del certificado.

IV.3 Reglas de confianza para firmas longevas.

1. En el caso de firmas longevas, el firmante o el verificador de la firma incluirá un sello de tiempo que permita garantizar que el certificado era válido en el momento en que se realizó la firma. En el caso de que sea incluida por el firmante, se podrá realizar una vez haya trascurrido el periodo de precaución o periodo de gracia.

2. Para la conversión de una firma electrónica a firma electrónica longeva:

a) Se verificará la firma electrónica, validando la integridad de la firma acorde a las reglas de validación de firma de electrónica del epígrafe III.7.

b) Se realizará un proceso de completado de la firma electrónica que consistirá en la obtención y almacenamiento de las referencias a:

i. Certificados: Incluyendo los certificados del firmante y de la cadena de certificación tanto del firmante como del sello de tiempo.

ii. Informaciones de estado de los certificados, CRLs o las respuestas OCSP.

c) Aplicación del sellado de tiempo a las referencias a los certificados y a las informaciones de estado.

3. Para la incorporación a la firma de la información completa de validación, se usará validación mediante CRLs u OCSP.

4. Las políticas de firma y sello contemplarán la definición de formatos y consideraciones de uso de firmas longevas conforme a las necesidades específicas de su ámbito de aplicación y a la normativa específica aplicable.

§ 32

Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 178, de 26 de julio de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-10049

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la norma relativa a la intermediación de datos responde a lo previsto en el artículo 9 de la Ley 11/2007, de 22 de junio, y en el artículo 8 del citado Real Decreto 4/2010, de 8 de enero, sobre el acceso y utilización de servicios de intercambio de datos y documentos entre Administraciones Públicas; definiendo un modelo para el intercambio intermediado de datos. Los intercambios intermediados constituyen un modelo recomendado internacionalmente tanto por la UE, como por la OCDE o la ONU, dada su demostrada eficiencia como herramienta de interoperabilidad en tanto que permite la normalización y reutilización de los servicios de intercambio.

En particular, la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos, en primer lugar y con carácter general, define los roles de los agentes que participan en los intercambios intermediados de datos; y, en segundo lugar, establece las condiciones relativas a los procesos de intercambio intermediado de datos a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas, condiciones asimismo aplicables a plataformas de intermediación de otras Administraciones Públicas.

Dichos roles y condiciones se establecen en términos de interoperabilidad tecnológica y se aplicarán junto a las consideraciones que correspondan a la naturaleza de la información objeto del intercambio o cesión de datos, de conformidad con la legislación que resulte de aplicación.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Norma Técnica de Interoperabilidad de Protocolos de Intermediación de Datos

I. Disposiciones generales

I.1 Objeto.

La Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos tiene por objeto establecer las especificaciones para el intercambio intemediado de datos entre Administraciones Públicas, o Entidades de Derecho Público vinculadas o dependientes de aquellas (en adelante, organizaciones).

I.2 Ámbito de aplicación.

1. El contenido de esta norma será de aplicación para el intercambio intermediado de datos a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

2. Las condiciones establecidas en esta norma relativas a los agentes participantes en los intercambios intermediados de datos se aplicarán en otras plataformas de intermediación en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

3. Las condiciones establecidas en esta norma relativas a la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas podrán aplicarse en el intercambio intermediado de datos a través de otras plataformas de intermediación en el ámbito referido en el apartado 2.

4. Las condiciones establecidas en esta norma se podrán aplicar en intercambios de datos no intermediados así como en otros nodos de interoperabilidad.

II. Agentes en los intercambios intermediados de datos

II.1 Cedente y Emisor.

1. Un Cedente será cualquier organización que posea datos relativos a los ciudadanos que otra pueda necesitar consultar en el ámbito del ejercicio de sus competencias; es el responsable de los mismos según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y los ofrecerá a posibles Cesionarios a través de un Emisor.

2. Un Emisor será el que facilita la cesión de los datos desde un punto de vista tecnológico.

3. Un Cedente que facilita la cesión de sus propios datos actuará, en el ámbito de esta norma, como Emisor a la vez de ser Cedente.

4. Cualquier nodo de interoperabilidad que participe en la gestión de los trámites de emisión o cesión de datos de un Emisor, tomará también el rol de Emisor en el ámbito de esta norma, incluyendo las funciones relacionadas con la firma electrónica de las comunicaciones que realiza.

5. Rol del Cedente:

a) Facilitará la información para el catálogo o registro de sus servicios de intercambio de datos disponibles bajo servicios de intercambio a disposición de otras organizaciones para su consulta.

b) Respecto a las autorizaciones de acceso a los servicios:

b.1) Establecerá los protocolos y condiciones de acceso a los servicios de intercambio de datos que ofrecen, los métodos de consulta permitidos así como la información a conocer de cada Requirente.

b.2) Justificará los casos de rechazo o denegación de una solicitud.

b.3) Definirá la política de auditoría y realizará auditorías periódicas sobre el uso del sistema relativo a las consultas de sus datos.

c) Podrá delegar estas tareas en el Emisor o en un nodo de interoperabilidad.

6. Rol del Emisor:

a) Establecerá las condiciones técnicas de acceso a los servicios de intercambio de datos que ofrece, los métodos de consulta permitidos y los controles y auditoría técnica, pudiendo delegar la ejecución de dichas condiciones en un nodo de interoperabilidad.

b) Definirá los controles y criterios de acceso a los datos necesarios para garantizar la confidencialidad de la información: políticas y procedimientos de gestión y control de acceso de usuarios y órganos.

c) Proporcionará los datos pertinentes a cada consulta con garantía de integridad y confidencialidad.

d) Informará sobre la disponibilidad de cada servicio de intercambio bajo su responsabilidad, así como sobre los mecanismos de soporte y resolución de incidencias disponibles en cada caso, incluyendo los datos de contacto para dichos servicios.

e) Definirá Acuerdos de Nivel de Servicio (ANS) para regular las condiciones de prestación de los servicios y mecanismos de respuesta a incidencias específicos acorde a la criticidad del servicio que se está prestando.

f) Mantendrá la traza de todas las peticiones recibidas y respuestas generadas.

II.2 Cesionario y Requirente.

1. Un Cesionario será cualquier organización autorizada a consultar determinados datos de los ciudadanos en poder de un Cedente.

2. Un Requirente será el que facilita la consulta de los datos desde un punto de vista tecnológico.

3. Un Cesionario que realiza directamente la consulta de datos actuará, en el ámbito de esta norma, como Requirente a la vez de ser Cesionario.

4. Cualquier nodo de interoperabilidad que participe en la gestión de los trámites de consulta de datos de un Requirente, tomará también el rol de Requirente en el ámbito de

esta norma, incluyendo las funciones relacionadas con la firma electrónica de las comunicaciones.

5. Rol del Cesionario:

a) Solicitará información siempre en relación con los trámites y procedimientos autorizados por el cedente y dentro del marco de un procedimiento administrativo.

b) Cumplirá las condiciones de acceso a los datos establecidas por el Cedente.

c) Recabará el consentimiento del interesado, salvo que una ley le exima de ello, y reflejará la respuesta obtenida del sistema, en el ámbito del expediente correspondiente.

d) Utilizará la información obtenida de cada consulta para la finalidad que corresponda en cada caso, realizando una misma consulta tantas veces como sea necesario y lo requiera el trámite a que se refiera la consulta, asumiendo expresamente la responsabilidad que pudiera derivar de posibles incumplimientos.

e) Colaborará en las labores de auditoría cuando sea requerido para ello, facilitando al Cedente la información o documentos necesarios para el control de las consultas.

6. Rol del Requirente:

a) Cumplirá las condiciones de acceso a los datos establecidas por el Emisor.

b) Asegurará que las peticiones de consulta contienen los datos de identificación, la información solicitada y la especificación del trámite o procedimiento en el que los datos serán usados y, si procede, los datos del Cesionario.

c) Mantendrá la traza de las peticiones que realiza y de las respuestas recibidas.

d) Colaborará en las labores de auditoría cuando sea requerido para ello.

e) Realizará las labores de monitorización y control necesarias para mantener un correcto funcionamiento de su servicio de consulta.

f) Asegurará las máximas garantías de seguridad y confidencialidad de las consultas, preservando la privacidad de los datos consultados tanto en el propio intercambio como en el tratamiento posterior de la información obtenida. Para ello, establecerá controles de autorización, acceso y uso por parte de los usuarios a las diferentes aplicaciones, mantendrá actualizados los datos de los usuarios y aplicaciones que acceden al sistema, notificando cualquier cambio de estado y asegurando la tramitación de su baja cuando corresponda.

g) No almacenará información personal de ningún ciudadano salvo la imprescindible para el trámite que se solicita, para la organización en nombre de la cual ha sido recabada y sólo durante el tiempo imprescindible.

III. Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas

III.1 Funciones.

1. El Ministerio de Hacienda y Administraciones Públicas funcionará como un nodo de interoperabilidad mediante la plataforma de Intermediación que, atendiendo a la definición de nodo de interoperabilidad recogida en el Real Decreto 4/2010, de 8 de enero, prestará funcionalidades comunes para el intercambio de información entre Emisores y Requirentes.

2. Rol de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas:

a) Gestionará los Cesionarios y Requirentes según las condiciones establecidas por cada Cedente.

b) No almacenará información personal de ningún ciudadano derivada de cualquier transacción de intercambio de datos.

c) Asegurará la confidencialidad e integridad de la información intercambiada a través de los mecanismos correspondientes.

d) Mantendrá un portal web informativo con toda la documentación relativa a la Plataforma, donde publicará al menos:

d.1) El catálogo de servicios de intercambio de datos disponibles por parte de las diferentes organizaciones, incluyendo: los protocolos de acceso a dichos servicios, los métodos de consulta permitidos, la información técnica relevante, así como la información que se requiere de cada Requirente.

d.2) Formularios de solicitud de acceso a los servicios.

d.3) Acuerdos de prestación de cada servicio disponible y de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas en general.

d.4) Novedades del servicio prestado por la Plataforma.

e) Mantendrá el sistema en funcionamiento 24x7.

f) Dará soporte a las organizaciones y gestionará todas las comunicaciones e incidencias producidas colaborando para ello con Requirentes y Emisores.

g) Mantendrá un centro de atención a usuarios e integradores que canalice todas las incidencias relativas al sistema e informará sobre los datos de contacto del mismo.

h) Elaborará informes de actividad y uso de la Plataforma considerando las consultas realizadas desde y hacia cada organización.

i) Evolucionará y mantendrá sus sistemas garantizando la seguridad y privacidad de los datos acorde a la normativa aplicable.

j) Colaborará en las labores de auditoría siempre que el Emisor o el Cedente así lo requiera y defina, conservando los datos de trazabilidad y estadísticos acordados, proporcionando acceso a los mismos cuando sea necesario y permitiendo reproducir la secuencia de operaciones llevadas a cabo por el sistema.

III.2 Gobernanza del sistema.

1. Cualquier organización podrá acceder a información sobre servicios de intercambio de datos disponibles a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas o, en su caso, a través del correspondiente nodo de interoperabilidad.

2. La incorporación de nuevos servicios en la Plataforma de Intermediación se coordinará entre el Ministerio de Hacienda y Administraciones Públicas y el organismo cedente correspondiente.

En el caso de servicios comunes ofrecidos por las CCAAs, la incorporación de nuevos servicios se aprobará previamente en el Comité Sectorial de Administración Electrónica.

3. Para el acceso a un servicio de intercambio de datos:

a) El Requirente enviará al Emisor la solicitud de alta para el acceso al servicio aplicando el formulario del anexo 1 a través de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas. Esta operación se realizará para cada Cesionario que gestione el Requirente.

b) El Emisor remitirá al Requirente la autorización del cesionario en respuesta a dicha solicitud. Dicha autorización contemplará la justificación de la legitimidad y competencia del Requirente y será registrada por la Plataforma de intermediación.

4. Las funciones de cada agente involucrado en la autorización podrán ser realizadas por la propia Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas o, en su caso, por un nodo de interoperabilidad que haya subscrito el correspondiente convenio con este Ministerio a tal efecto.

III.3 Requisitos técnicos.

1. La Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas garantizará la interoperabilidad, disponibilidad, fiabilidad y seguridad de la información transmitida a través de ella entre las diferentes organizaciones con las que interactúa.

2. En el acceso a la Plataforma de intermediación de datos del Ministerio de Hacienda y Administraciones Públicas se utilizará la Red de comunicaciones de las Administraciones públicas españolas atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas.

III.4 Aspectos generales de seguridad.

El intercambio de datos entre la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas y las organizaciones se realizará en unas condiciones tales que garanticen la seguridad de la información que se transmite, proporcionando medidas para la

autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad adecuadas a la naturaleza de la misma:

a) Autenticidad. Se asegurará la identidad de todos los agentes que intervengan en el proceso de intercambio de datos, de forma que todos ellos estén correctamente identificados en cada intercambio. Para ello, se aplicarán las medidas de seguridad contempladas en el Real Decreto 3/2010, de 8 de enero, dentro del grupo «marco operacional» en el capítulo relativo a «Control de acceso» (op.acc); y del grupo «medidas de protección», en el capítulo «Protección de la información» (mp.info).

b) Confidencialidad e integridad de la información intercambiada, que será protegida conforme al grupo de «medidas de protección», capítulos «Protección de las comunicaciones» (mp.com) y «Protección de la información» (mp.info) definidas en el Real Decreto 3/2010, de 8 de enero, y con las medidas de seguridad dispuestas en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, asegurando que no se almacena información personal de ningún ciudadano.

c) Disponibilidad de la Plataforma, asegurada a través de medidas establecidas en el capítulo «Protección de los servicios» (mp.$) del grupo de «medidas de protección» definidas en el Real Decreto 3/2010, de 8 de enero.

d) Trazabilidad, según lo establecido en el apartado 111.6 de esta norma.

III.5 Tecnologías y estándares.

1. Las tecnologías utilizadas para los intercambios se implementarán en base a estándares abiertos e interoperables según lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

2. Los intercambios de información se podrán implementar a través de servicios web, que, como conjunto de protocolos y estándares abiertos sobre los que desarrollar estructuras de datos específicas para cada tipo de intercambio, incorporarán los mecanismos de seguridad necesarios para la comunicación.

3. Los servicios web implementados se diseñarán en base a la utilización de:

a) Servicios definidos mediante un lenguaje WSDL *(Web Services Description Language).*

b) Mensajes en formato XML (eXtensible Mark-up Language) con estructuras basadas en esquemas XML publicados que faciliten su interpretación.

c) Estándares de seguridad en las comunicaciones a nivel de transporte punto a punto, mediante el uso del protocolo TLS *(Transport Layer Security)* con autenticación de cliente a nivel de transporte, o a nivel de aplicación mediante el uso de protocolos que garanticen la seguridad extremo a extremo en servicios Web.

4. De forma general en servicios de intercambio se utilizará la versión 3.0 del protocolo SCSP (Sustitución de Certificados en Soporte Papel) cuya especificación está disponible en el Portal de Administración electrónica PAE/CTT en la dirección http://administracionelectronica.gob.es/es/ett/sesp.

Se podrá utilizar la versión 2 del protocolo SCSP en servicios ya existentes que no requieran mecanismos adicionales de seguridad sin perjuicio de que exista una versión actualizada del mismo servicio.

III.6 Trazabilidad y auditoría de los intercambios.

1. Emisores y Requirentes mantendrán trazabilidad de los intercambios de datos producidos, para lo cual podrán apoyarse en funcionalidades prestadas por la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas, y en lo previsto sobre trazabilidad en el Real Decreto 3/2010, de 8 de enero.

2. La conservación de trazas por parte de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas, establecida atendiendo a las medidas de seguridad contempladas en el Real Decreto 3/2010, de 8 de enero: op.exp.10 «Protección de los registros de actividad», op.exp.8 «Registro de la actividad de los usuarios», mp.info.5 «Sellos de tiempo», facilitará la auditoría de los intercambios. La información aportada por la Plataforma se completará con aquella que permita la recuperación de los datos específicos intercambiados que conservarán Emisor y Requirente.

3. La Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas no almacenará información sobre el contenido del intercambio ni asumirá funciones relativas a la conservación de trazas y auditoría, mas allá de lo establecido en el apartado 111.6 y en cuyo caso la definición de funciones y mecanismos de puesta a disposición del agente interesado será documentada convenientemente. El Cedente podrá auditar la cesión de datos para comprobar el cumplimiento de los requisitos a que pudiera ésta estar sujeta.

4. Para garantizar la trazabilidad de los intercambios producidos, se asociará a cada petición o consulta un identificador único que permitirá reproducir la secuencia de operaciones llevadas a cabo.

5. La información almacenada para la trazabilidad de cada consulta o intercambio contemplará, al menos, lo siguiente:

a) Identificador de la transacción.

b) Cesionario de la información, Requirente que la solicita y usuario final que la realiza especificando, si es posible, el empleado público o aplicación.

c) Tipo de información que se solicita.

d) Fecha y hora de realización de la consulta.

III.7 Catálogo de servicios de intercambio de datos.

1. El catálogo o registro de los servicios de intercambio de datos ofrecidos por cada Cedente será incorporado al catálogo de la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas sirviendo de referencia a posibles Requirentes.

2. El catálogo de servicios de intercambio de datos estará disponible para su consulta por las distintas organizaciones a través de alguno de los siguientes medios:

a) Un punto informativo propio del Cedente o del Emisor, si se delega en éste por parte del Cedente, que podrá ser su sede electrónica.

b) La Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas.

c) Los instrumentos para la interoperabilidad establecidos en el Real Decreto 4/2010, de 8 de enero:

i. Inventario de procedimientos administrativos y servicios prestados.

ii. Centro de Interoperabilidad Semántica de la Administración.

3. En el catálogo o registro de servicios figurará, para cada servicio disponible o supuesto genérico de intercambio, al menos, la información general definida en el anexo 11.

4. Para la publicación de nuevos servicios en la Plataforma de intermediación del Ministerio de Hacienda y Administraciones Públicas se podrá utilizar UDDI (Universal Description, Discovery and Integration) o un servicio de directorio como medio para facilitar el descubrimiento dinámico de nuevos servicios, aunque el uso de aquellos dependerá en cualquier caso de la formalización de las autorizaciones necesarias correspondientes.

§ 33

Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 178, de 26 de julio de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-10050

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la norma relativa a la publicación de modelos de datos responde a lo previsto en el artículo 10 del citado Real Decreto 4/2010, de 8 de enero, sobre activos semánticos.

En particular, la Norma Técnica de Interoperabilidad de Relación de modelos de datos define las condiciones para establecer y publicar los modelos de datos a los que se refiere el citado artículo 10 relativas al formato, identificación y documentación asociada a los modelos de datos, a sus posibles usos así como a sus definiciones y codificaciones asociadas, al objeto de facilitar la interacción con el Centro de Interoperabilidad Semántica, encargado de su publicación. Este modelo de intercambio y publicación de modelos de datos está alineado

con prácticas y estándares reconocidos a nivel europeo promovidos desde SEMIC.EU: Semantic Interoperability Centre Europe.

En cuanto a las definiciones y codificaciones asociadas a los modelos de datos, atendiendo al epígrafe cuatro del citado artículo 10, la norma establece las condiciones para que, aquellas de interés estadístico, tengan en cuenta los modelos estándares establecidos por el Instituto Nacional de Estadística con el fin de asegurar la aplicación de sistemas normalizados de conceptos, definiciones, unidades estadísticas, clasificaciones, nomenclaturas y códigos que hagan factible la comparación, la integración y el análisis de los datos y los resultados obtenidos, tal y como establece la Ley 12/1989, de 9 de mayo, de la Función estadística pública. Por otra parte, la norma establece el uso de la codificación de Unidades Orgánicas y Oficinas de la Administración a través del Directorio Común gestionado por el Ministerio de Hacienda y Administraciones Públicas para la descripción de los modelos de datos.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Relación de modelos de datos cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Relación de modelos de datos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE RELACIÓN DE MODELOS DE DATOS

I. Objeto

La Norma Técnica de Interoperabilidad de Relación de modelos de datos tiene por objeto definir las condiciones para establecer y publicar modelos de datos que tengan el carácter de comunes en la Administración y aquellos que se refieran a materias sujetas a intercambio de información con los ciudadanos y otras administraciones, así como las definiciones y codificaciones asociadas, de cara a su publicación en el Centro de Interoperabilidad Semántica.

II. Ámbito de aplicación

El contenido de esta norma será de aplicación en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

III. Modelos de datos a publicar

Los órganos de la Administración pública y las Entidades de Derecho Público vinculadas o dependientes de aquélla establecerán y compartirán, junto a las definiciones y codificaciones asociadas, los modelos de datos de los que sean titulares y se refieran a:

a) Materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas.

b) Infraestructuras, servicios y herramientas comunes, que no sean de uso exclusivamente interno a la organización.

IV. Estructura de intercambio de los modelos de datos

Los modelos de datos a publicar en el Centro de Interoperabilidad Semántica (CISE) se ajustarán a la estructura de intercambio definida en el anexo I conteniendo:

a) Activos semánticos, en formato XSD (XML Schema Definition), clasificados según los servicios ó unidades de negocio de las diferentes administraciones.

b) Guías explicativas, en formato PDF (Portable Document Format), atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares, de los diferentes servicios ó sistemas de intercambio, que incluirán:

i. Descripción de los tipos y definiciones de datos que se intercambian bajo el modelo de datos de que se trate, así como una descripción funcional de las operaciones que se pueden realizar.

ii. Breve descripción de las condiciones de seguridad aplicables a los intercambios con dicho modelo.

iii. Condiciones que deben cumplir lo receptores de la información a la que aplica el modelo en cuestión.

iv. Ejemplos de implementación de los diferentes servicios bajo el modelo de datos que corresponda.

v. De forma opcional, manuales de ayuda del servicio de intercambio y juegos de pruebas.

V. Identificación de los modelos de datos

V.1 Los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla proporcionarán una identificación de la estructura de intercambio de sus modelos de datos, que permitirá su clasificación y facilitará al Centro de Interoperabilidad Semántica las tareas de identificación, localización y clasificación de los modelos de datos cuya publicación centraliza.

V.2 La información para la identificación de los modelos de datos incluirá, al menos, los datos descritos en el anexo II.

V.3 La descripción de los modelos de datos se ajustará a los estándares establecidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

V.4 Para darse de alta en el Centro de Interoperabilidad Semántica, el órgano responsable de los modelos de datos remitirá un mensaje por correo electrónico a la dirección « admin.cise@seap.minhap.es», que antepondrá como asunto del mismo el encabezamiento «ALTA CISE» + «Identificador Normalizado de órgano extraído del Directorio Común de Organismos y Oficinas gestionado por el MINHAP» y contendrá en el cuerpo del mensaje la siguiente información: «Nombre del organismo emisor», «Dirección URL», «Dirección de correo electrónico».

VI. Interacción con el Centro de Interoperabilidad Semántica

Para su interacción con el Centro de Interoperabilidad Semántica, cada órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquélla:

a) Identificará los modelos de datos susceptibles de ser intercambiados con el Centro de Interoperabilidad Semántica, atendiendo a lo establecido en el apartado V de la presente norma técnica.

b) Facilitará la estructura de intercambio de los modelos de datos al Centro de Interoperabilidad Semántica mediante uno de los siguientes procedimientos, asegurando en cualquier caso la actualización de la información facilitada:

i. Recopilación y depósito de los modelos de datos, estructurados según el apartado IV, en un entorno de intercambio accesible por el Centro de Interoperabilidad Semántica a

través de la Red de comunicaciones de las Administraciones públicas españolas, para su carga masiva.

Dicho entorno será convenientemente identificado a través de la correspondiente URL (Uniform Resource Locator) definida por el propietario del modelo de datos y que atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

ii. Publicación de cada modelo de datos directamente a través de las herramientas que disponga el Centro de Interoperabilidad Semántica y atendiendo al procedimiento de utilización que éste establezca.

c) Actualizará de manera proactiva la información facilitada al Centro de Interoperabilidad Semántica, bien a través del entorno de intercambio o a través de las herramientas que el Centro de Interoperabilidad Semántica establezca a tal efecto.

d) Podrá consultar los modelos de datos disponibles en el repositorio de información del Centro de Interoperabilidad Semántica y recibir notificaciones automáticas de dicho Centro ante la publicación y actualización de modelos de datos.

VII. Uso de los modelos de datos

VII.1 Los modelos de datos comunes publicados en el Centro de Interoperabilidad Semántica serán de preferente aplicación según lo establecido en el artículo 10.1 del Real Decreto 4/2010, de 8 de enero.

VII.2 Los modelos de datos de titulares de competencias en materias sujetas a intercambio de información con los ciudadanos y con otras Administraciones públicas, así como en materia de infraestructuras, servicios y herramientas comunes publicados en el Centro de Interoperabilidad Semántica serán de obligatoria aplicación según lo establecido en el artículo 10.2 del Real Decreto 4/2010, de 8 de enero.

VII.3 El Centro de Interoperabilidad Semántica identificará convenientemente los modelos de datos comunes de obligatoria aplicación, diferenciándolos de otros modelos de datos aportados por las diferentes administraciones.

VII.4 En el Comité Sectorial de Administración Electrónica se identificarán, catalogarán y priorizarán los modelos de datos comunes.

VIII. Codificaciones

VIII.1 Las definiciones y codificaciones de interés estadístico:

a) Serán aquellas que dispongan de un modelo estándar definido por el Instituto Nacional de Estadística disponible en el portal del Instituto y en el Centro de Interoperabilidad Semántica.

b) Serán identificadas en los modelos de datos de las que formen parte según lo dispuesto en el apartado V de esta norma.

c) Ante su presencia en nuevos modelos o en actualizaciones de modelos de datos existentes publicados en el Centro de Interoperabilidad Semántica, podrán ser contrastadas por el Instituto Nacional de Estadística con sus modelos estándar.

En caso de que dichos modelos de datos no se ajusten a los modelos estándar definidos, el Instituto Nacional de Estadística lo pondrá en conocimiento del Ministerio de Hacienda y Administraciones Públicas, quien lo pondrá en conocimiento de la Administración o Entidad responsable a los efectos oportunos.

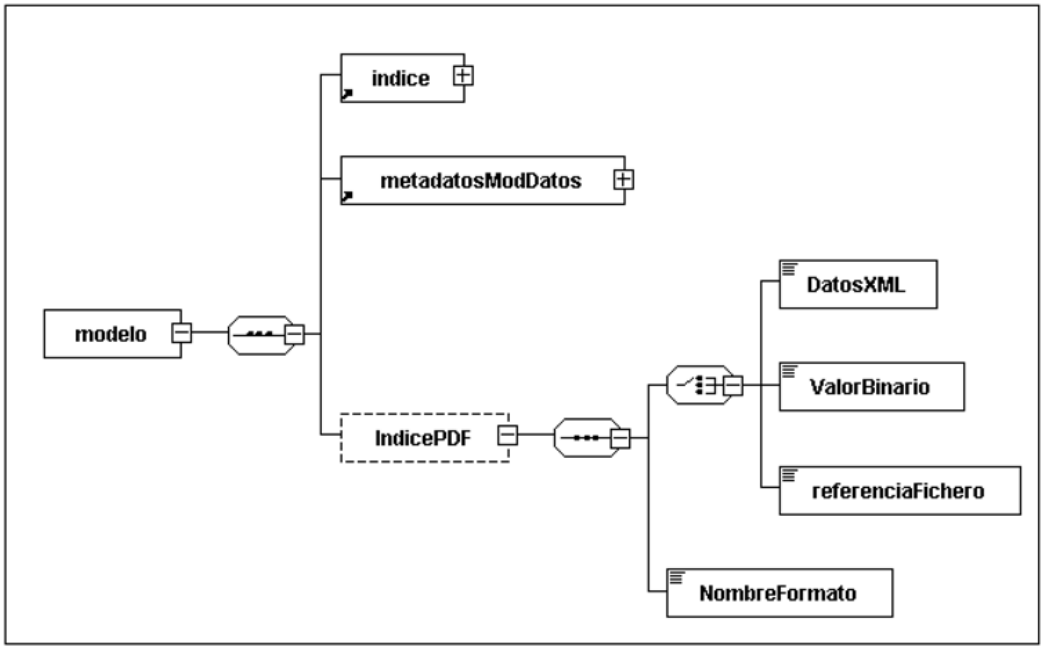
VIII.2 La codificación de Unidades Orgánicas y Oficinas de la Administración en los modelos de datos aplicará las establecidas en el Directorio Común de Organismos y Oficinas, que será gestionado por el Ministerio de Hacienda y Administraciones Públicas y alimentado por todos los órganos de la Administración pública o Entidades de Derecho Público vinculadas o dependientes de aquélla.

El Centro de Interoperabilidad Semántica publicará toda la documentación de integración, procedimientos de colaboración, y definición de atributos de la información del Directorio, teniendo en cuenta lo recogido en esta norma sobre intercambio de modelos de datos. Asimismo, dicho Centro publicará y mantendrá actualizada una relación de las fuentes colaboradoras y un enlace a la aplicación de gestión del Directorio Común.

ANEXO I

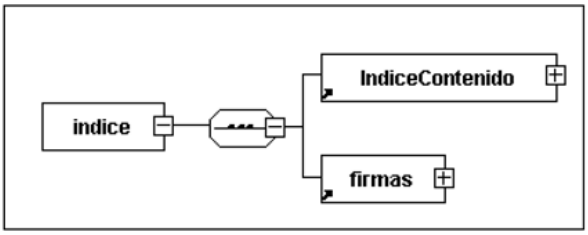
Esquemas XML para publicación de modelos de datos

1. *XSD Modelo de datos*



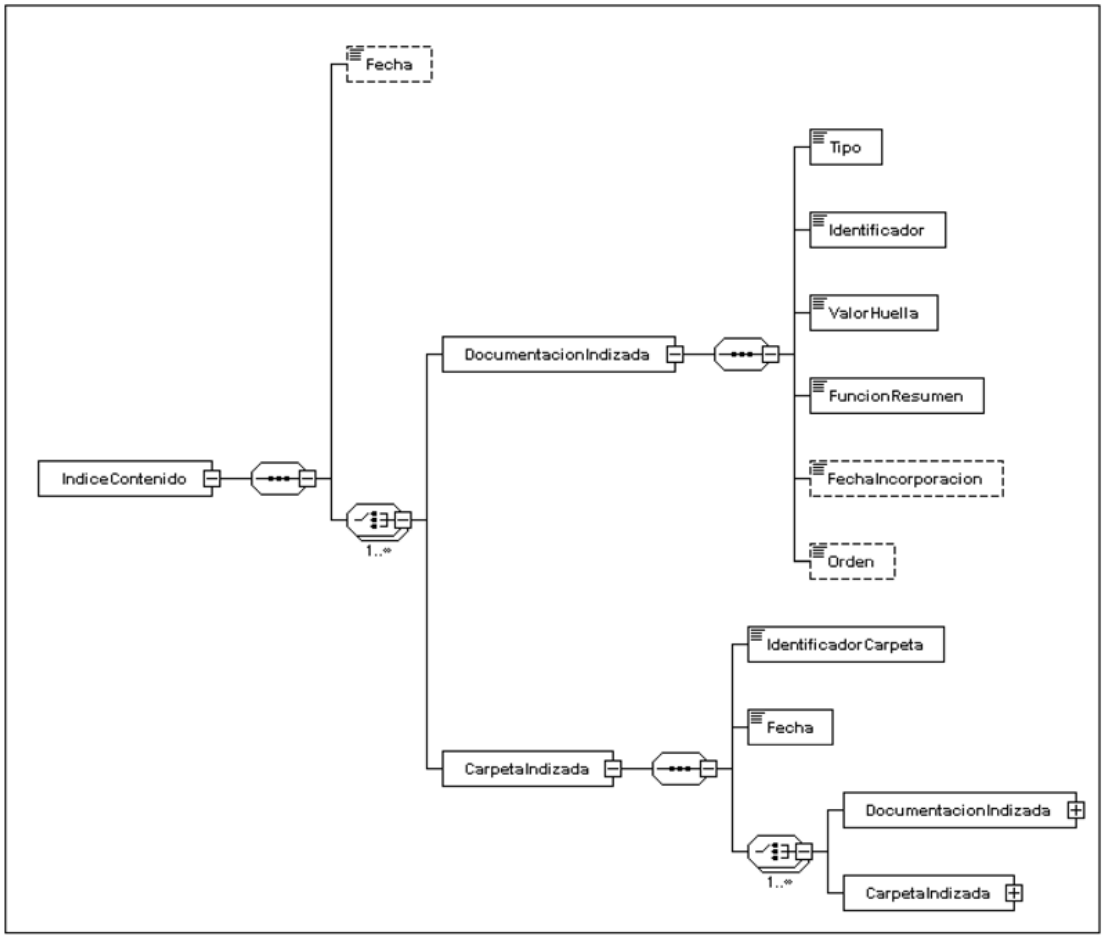

```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ModDatosInd="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice"
xmlns:ModDatosMeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos"
xmlns:ModDatos="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD MODELOS DE DATOS versión 1.0 - 25/10/2011.</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/IndiceModDatos.xsd" />
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos/MetadatosModDatos.xsd" />
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido/contenidoDocumentoEni.xsd" />
<xsd:element name="modelo" type="ModDatos:TipoModelo" />

<xsd:complexType name="TipoModelo">
        <xsd:sequence>
                <xsd:element ref="ModDatosInd:indice" />
                <xsd:element ref="ModDatosMeta:metadatosModDatos" />
                <xsd:element name="IndicePDF" type="enifile:TipoContenido" minOccurs="0" />
        </xsd:sequence>
         <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
</xsd:schema>
```

2. *XSD Índice del modelo de datos*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma"
xmlns:ModDatosInd="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice"
xmlns:ModDatosIndcon="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD INDICE MODELO DE DATOS versión 1.0 - 25/10/2011.</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma/firmasEni.xsd" />
<xsd:import namespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido" schemaLocation="
http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido/IndiceModDatosCon.xsd" />
<xsd:element name="indice" type="ModDatosInd:TipoIndice" />

<xsd:complexType name="TipoIndice">
        <xsd:sequence>
                <xsd:element ref="ModDatosIndcon:IndiceContenido" />
                <xsd:element ref="enids:firmas" />
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

</xsd:schema>
```

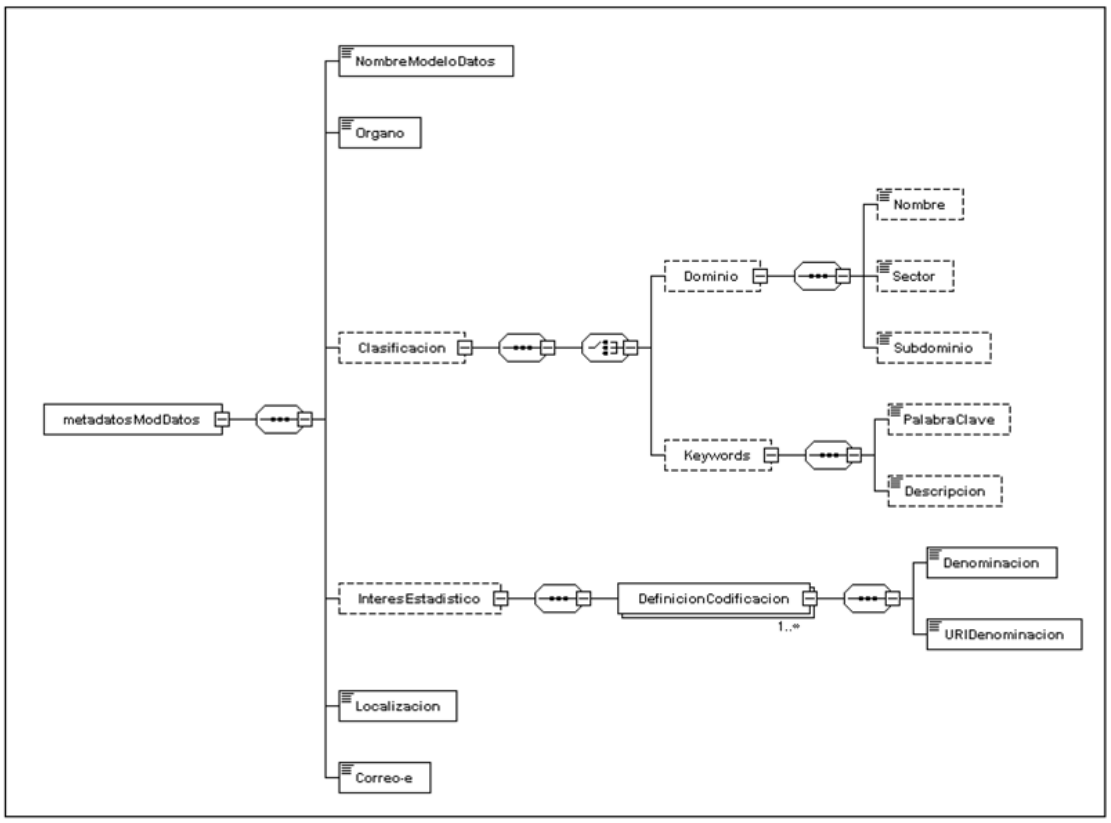
3. *XSD Contenido del índice del modelo de datos*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ModDatosIndcon="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/indice/contenido" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD CONTENIDO INDICE MODELO DE DATOS version 1.0 -
        25/10/2011.</xsd:documentation>
</xsd:annotation>
```

```
<xsd:element name="IndiceContenido" type="ModDatosIndcon:TipoIndiceContenido" />
<xsd:complexType name="TipoIndiceContenido">
	<xsd:sequence>
		<xsd:element name="Fecha" type="xsd:dateTime" minOccurs="0" />
		<xsd:choice maxOccurs="unbounded">
			<xsd:element name="DocumentacionIndizada" type="ModDatosIndcon:TipoIndizado" />
			<xsd:element name="CarpetaIndizada" type="ModDatosIndcon:TipoCarpetaIndizada" />
		</xsd:choice>
	</xsd:sequence>
	<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

<xsd:complexType name="TipoIndizado">
	<xsd:sequence>
		<xsd:element name="Tipo" type="xsd:boolean">
			<xsd:annotation>
				<xsd:documentation xml:lang="es">0-Documentacion complementaria. 1-Modelo de datos
				(XSD).</xsd:documentation>
			</xsd:annotation>
		</xsd:element>
		<xsd:element name="Identificador" type="xsd:string" />
		<xsd:element name="ValorHuella" type="xsd:string" />
		<xsd:element name="FuncionResumen" type="xsd:string" />
		<xsd:element name="FechaIncorporacion" type="xsd:dateTime" minOccurs="0" />
		<xsd:element name="Orden" type="xsd:string" minOccurs="0" />
	</xsd:sequence>
	<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

<xsd:complexType name="TipoCarpetaIndizada">
	<xsd:sequence>
		<xsd:element name="IdentificadorCarpeta" type="xsd:string" />
		<xsd:element name="Fecha" type="xsd:dateTime" />
		<xsd:choice maxOccurs="unbounded">
			<xsd:element name="DocumentacionIndizada" type="ModDatosIndcon:TipoIndizado" />
			<xsd:element name="CarpetaIndizada" type="ModDatosIndcon:TipoCarpetaIndizada" />
		</xsd:choice>
	</xsd:sequence>
	<xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>
</xsd:schema>
```

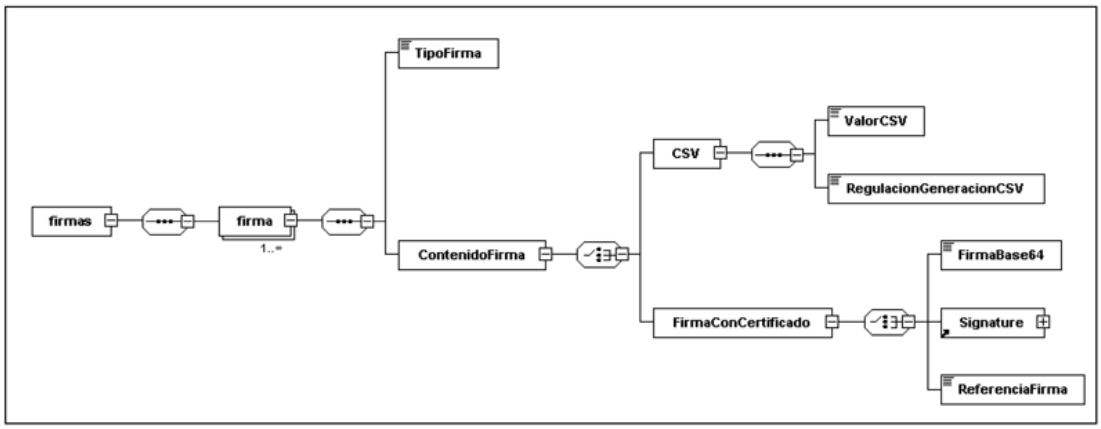
4. *XSD Metadatos del modelo de datos*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:ModDatosMeta="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/ModDatos/metadatos" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD METADATOS MODELOS DE DATOS versión 1.0 -
        25/10/2011.</xsd:documentation>
</xsd:annotation>
```

```
<xsd:element name="metadatosModDatos" type="ModDatosMeta:TipoMetadatos" />

<xsd:complexType name="TipoMetadatos">
        <xsd:sequence>
                <xsd:element name="NombreModeloDatos" type="xsd:string" />
                <xsd:element name="Organo" type="xsd:string" >
                        <xsd:annotation>
                                <xsd:documentation xml:lang="es"> Código alfanumérico único para cada órgano/unidad/oficina
                                extraído del Directorio Común gestionado por el Ministerio de Hacienda y Administraciones
                                Públicas.</xsd:documentation>
                        </xsd:annotation>
                </xsd:element >
                <xsd:element name="Clasificacion" type="ModDatosMeta:TipoClasificacion" minOccurs="0" />
                <xsd:element name="InteresEstadistico" type="ModDatosMeta:TipoInteresEstadistico" minOccurs="0"
                maxOccurs="1">
                        <xsd:annotation>
                                <xsd:documentation xml:lang="es"> Identificación unívoca de la definición y codificación de
                                interés estadístico del modelo de datos definida por el Instituto Nacional de
                                Estadística.</xsd:documentation>
                        </xsd:annotation>
                </xsd:element >
                <xsd:element name="Localizacion" type="xsd:anyURI" />
                 <xsd:element name="Correo-e" type="xsd:string" />
         </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional" />
</xsd:complexType>

<xsd:complexType name="TipoClasificacion">
        <xsd:sequence>
                <xsd:choice>
                        <xsd:element name="Dominio" type="ModDatosMeta:TipoDominio" minOccurs="0" />
                        <xsd:element name="Keywords" type="ModDatosMeta:TipoKeywords" minOccurs="0" />
                </xsd:choice>
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TipoDominio">
        <xsd:sequence>
                <xsd:element name="Nombre" type="xsd:string" minOccurs="0" />
                <xsd:element name="Sector" type="xsd:string" minOccurs="0" />
                <xsd:element name="Subdominio" type="xsd:string" minOccurs="0" />
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TipoKeywords">
        <xsd:sequence>
                <xsd:element name="PalabraClave" type="xsd:string" minOccurs="0" />
                <xsd:element name="Descripcion" type="xsd:string" minOccurs="0" />
        </xsd:sequence>
 </xsd:complexType>

<xsd:complexType name="TipoInteresEstadistico">
        <xsd:sequence>
                <xsd:element name="DefinicionCodificacion" type="ModDatosMeta:TipoDefinicionCodificacion" minOccurs="1"
                maxOccurs="unbounded" />
         </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="TipoDefinicionCodificacion">
        <xsd:sequence>
                <xsd:element name="Denominacion" type="xsd:string" />
                <xsd:element name="URIDenominacion" type="xsd:anyURI" />
        </xsd:sequence>
 </xsd:complexType>
 </xsd:schema>
```

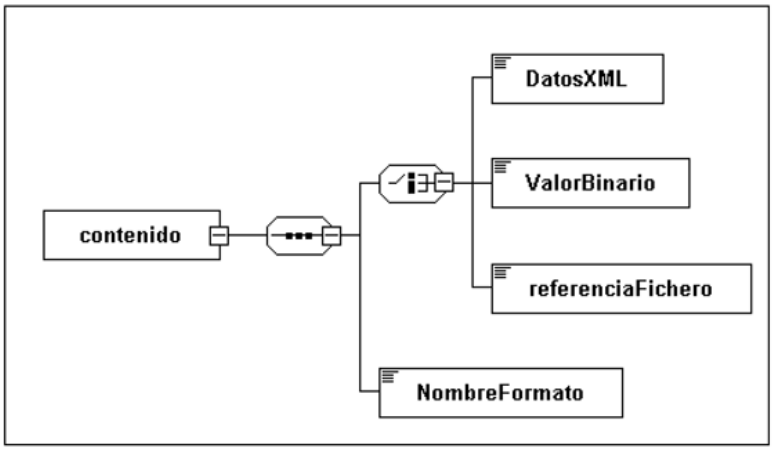
5. *XSD Firmas*




```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enids="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma " xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/firma " elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD FIRMAS ELECTRONICAS ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-
schema.xsd"/>
<xsd:element name="firmas" type="enids:firmas"/>
<xsd:complexType name="firmas">
        <xsd:sequence>
                <xsd:element name="firma" type="enids:TipoFirmasElectronicas" minOccurs="1" maxOccurs="unbounded"/>
        </xsd:sequence>
</xsd:complexType>
```

```
<xsd:complexType name="TipoFirmasElectronicas">
	<xsd:sequence>
		<xsd:element name="TipoFirma">
			<xsd:annotation>
				<xsd:documentation xml:lang="es">
					- TF01 - CSV.
					- TF02 - XAdES internally detached signature.
					- TF03 - XAdES enveloped signature.
					- TF04 - CAdES detached/explicit signature.
					- TF05 - CAdES attached/implicit signature.
					- TF06 - PAdES.
				</xsd:documentation>
			</xsd:annotation>
			<xsd:simpleType>
				<xsd:restriction base="xsd:string">
					<xsd:enumeration value="TF01"/>
					<xsd:enumeration value="TF02"/>
					<xsd:enumeration value="TF03"/>
					<xsd:enumeration value="TF04"/>
					<xsd:enumeration value="TF05"/>
					<xsd:enumeration value="TF06"/>
				</xsd:restriction>
			</xsd:simpleType>
		</xsd:element>
		<xsd:element name="ContenidoFirma">
			<xsd:complexType>
				<xsd:choice>
					<xsd:element name="CSV">
						<xsd:complexType>
							<xsd:sequence>
								<xsd:element name="ValorCSV" type="xsd:string"/>
								<xsd:element name="RegulacionGeneracionCSV"
								type="xsd:string"/>
							</xsd:sequence>
						</xsd:complexType>
					</xsd:element>
					<xsd:element name="FirmaConCertificado">
						<xsd:complexType>
							<xsd:choice>
								<xsd:element name="FirmaBase64"
								type="xsd:base64Binary"/>
								<xsd:element ref="ds:Signature"/>
								<xsd:element name="ReferenciaFirma">
									<xsd:annotation>
									<xsd:documentation  xml:lang="es">
									Referencia interna al fichero que incluye la firma.
									</xsd:documentation>
									</xsd:annotation>
								</xsd:element>
							</xsd:choice>
						</xsd:complexType>
					</xsd:element>
				</xsd:choice>
			</xsd:complexType>
		</xsd:element>
	</xsd:sequence>
<xsd:attribute name="Id" type="xsd:ID" use="optional"/>
<xsd:attribute name="ref" type="xsd:string" use="optional">
	<xsd:annotation>
		<xsd:documentation xml:lang="es">Almacena el identificador del nodo que se está firmando. En caso de firmas
		multinodo, se incluirá una lista separada por comas de los identificadores de los nodos firmados.
		</xsd:documentation>
	</xsd:annotation>
</xsd:attribute>
</xsd:complexType>
</xsd:schema>
```

6. *XSD Contenido de Documento electrónico*




```
<?xml version="1.0" encoding="UTF -8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:enifile="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
targetNamespace="http://administracionelectronica.gob.es/ENI/XSD/v1.0/documento-e/contenido"
elementFormDefault="qualified" attributeFormDefault="unqualified">
<xsd:annotation>
        <xsd:documentation xml:lang="es">XSD CONTENIDO DOCUMENTO ENI (v1.0)</xsd:documentation>
</xsd:annotation>
<xsd:element name="contenido" type="enifile:TipoContenido"/>
<xsd:complexType name="TipoContenido">
        <xsd:sequence>
                <xsd:choice>
                        <xsd:element name="DatosXML" type="xsd:anyType">
                                <xsd:annotation>
                                        <xsd:documentation xml:lang="es">Contenido en formato XML. En caso de datos XML
                                        cuya codificación difiera de la de esta estructura raiz se incluirá una cláusula
                                        CDATA.</xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                        <xsd:element name="ValorBinario" type="xsd:base64Binary">
                                <xsd:annotation>
                                        <xsd:documentation xml:lang="es">Contenido en base64.</xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                        <xsd:element name="referenciaFichero" type="xsd:string">
                                <xsd:annotation>
                                        <xsd:documentation xml:lang="es">Referencia interna al fichero de contenido.
                                        </xsd:documentation>
                                </xsd:annotation>
                        </xsd:element>
                </xsd:choice>
                <xsd:element name="NombreFormato" type="xsd:string">
                        <xsd:annotation>
                                <xsd:documentation xml:lang="es">El formato del fichero de contenido del documento
                                electrónico atenderá a lo establecido en la NTI de Catálogo de estándares.
                                </xsd:documentation>
                        </xsd:annotation>
                </xsd:element>
        </xsd:sequence>
        <xsd:attribute name="Id" type="xsd:ID" use="optional"/>
</xsd:complexType>
</xsd:schema>
```

ANEXO II

Identificación de los modelos de datos

Tabla 1. Identificación de los modelos de datos

Información	Descripción
Nombre	Nombre identificativo del modelo de datos.
Órgano	Identificador normalizado del órgano o entidad de la Administración que pone a disposición el activo, extraído del Directorio Común gestionado por el MINHAP.

Información	Descripción
Interés estadístico	Denominación de las definiciones y codificaciones de interés estadístico contenidas en el modelo.
Localización	Localización del servicio de intercambio tipo URI (Uniform Resource Identifier). En caso de estar disponible, localización del Servicio web correspondiente.
Correo-e de la unidad generadora	Correo electrónico de la unidad generadora de los modelos de datos, necesario para gestión en la comunicación con el Centro de Interoperabilidad Semántica.

§ 34

Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 178, de 26 de julio de 2012
Última modificación: sin modificaciones
Referencia: BOE-A-2012-10048

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: Documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos establece los conceptos relacionados con el desarrollo de políticas de gestión de documentos electrónicos, identifica los procesos de la gestión de documentos en el marco de la administración electrónica y establece los principios necesarios para el desarrollo y aplicación de políticas de gestión de documentos electrónicos por parte de todos los órganos de la Administración y Entidades de Derecho Público vinculadas o dependientes de aquélla.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la Disposición Transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos

I. Objeto

La Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos tiene por objeto establecer las directrices para la definición de políticas de gestión de documentos electrónicos.

II. Ámbito de aplicación

II.1 El contenido de esta norma será de aplicación para el desarrollo de políticas de gestión de documentos electrónicos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

II.2 Las directrices establecidas en esta norma se podrán aplicar en el desarrollo de políticas de gestión de documentos en entornos híbridos en que convivan documentos en soporte papel y documentos electrónicos.

III. Contenido y contexto

III.1 La política de gestión de documentos electrónicos será un documento que incluirá:

1. Definición del alcance y ámbito de aplicación.
2. Roles de los actores involucrados.
3. Directrices para la estructuración y desarrollo de los procedimientos de gestión documental.
4. Acciones de formación relacionada contempladas.
5. Actuaciones de supervisión y auditoría de los procesos de gestión de documentos.

6. Proceso de revisión del contenido de la política con el fin de garantizar su adecuación a la evolución de las necesidades de la gestión de documentos.

III.2 La política de gestión de documentos electrónicos:

1. Se integrará en el marco general de gestión de documentos y en el contexto de cada organización junto al resto de políticas implantadas para el desempeño de sus actividades.
2. Aplicará los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como los estándares y buenas prácticas nacionales e internacionales aplicables para la gestión documental atendiendo a lo establecido en la Norma Técnica de Interoperabilidad de Catálogo de estándares.

IV. Actores involucrados

Los actores involucrados en la definición, aprobación e implantación de la política de gestión de documentos electrónicos en una organización, serán, al menos, los siguientes:

1. La alta dirección que aprobará e impulsará la política.
2. Los responsables de procesos de gestión que aplicarán la política en el marco de los procesos de gestión a su cargo.
3. El personal responsable de la planificación, implantación y administración del programa de tratamiento de documentos y sus operaciones, cualificado, dedicado e instruido en gestión y conservación documental y que participará en el diseño, implementación y actualización de los sistemas de gestión y conservación documental.
4. El personal implicado en tareas de gestión de documentos electrónicos que aplicará lo establecido en la política a través del programa de tratamiento implantado.

V. Programa de tratamiento de documentos electrónicos

V.1 El diseño, desarrollo e implantación de los procesos, técnicas y operaciones de gestión de documentos electrónicos se concretará en un programa de tratamiento específico para la gestión de documentos y expedientes electrónicos.
V.2 Dicho programa de tratamiento se aplicará de manera continua sobre todas las etapas o periodos del ciclo de vida de los documentos y expedientes electrónicos para los que garantizará su autenticidad, integridad, confidencialidad, disponibilidad y trazabilidad; permitiendo la protección, recuperación y conservación física y lógica de los documentos y su contexto.

VI. Procesos de gestión de documentos electrónicos

Los procesos de gestión de documentos electrónicos de una organización incluirán, al menos, los siguientes:

1. Captura de documentos, que incluirá el tratamiento de los metadatos mínimos obligatorios definidos en la Norma Técnica de Interoperabilidad de Documento Electrónico.
2. Registro legal de documentos, definido en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común que, además del tratamiento de documentos electrónicos recibidos, atenderá a la posibilidad de digitalizar documentos en soporte papel según lo establecido en la Norma Técnica de Interoperabilidad de Digitalización de Documentos.
3. Clasificación de documentos, que incluirá los criterios de formación de expedientes y agrupaciones de documentos electrónicos según la Norma Técnica de Interoperabilidad de Expediente Electrónico, así como la clasificación funcional de acuerdo con el cuadro de clasificación de la organización.
4. Descripción de documentos, que atenderá a lo establecido en el apartado VII de esta norma así como a la posible redacción de un esquema institucional de metadatos.
5. Acceso a los documentos, que contemplará la posible regulación institucional de dicha práctica así como la trazabilidad de las acciones que se realizan sobre cada uno de ellos.
6. Calificación de los documentos, que incluirá:

i. Determinación de los documentos esenciales.

ii. Valoración de documentos y determinación de plazos de conservación.
iii. Dictamen de la autoridad calificadora.

7. Conservación de los documentos en función de su valor y tipo de dictamen de la autoridad calificadora, a través de la definición de calendarios de conservación.

8. Transferencia de documentos, que incluirá las consideraciones para la transferencia entre repositorios así como las responsabilidades en cuanto a su custodia.

9. Destrucción o eliminación de los documentos, que atenderá a la normativa aplicable en materia de eliminación de Patrimonio Documental y contemplará la aplicación de las medidas de seguridad relacionadas definidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica: Borrado y destrucción del capítulo de «Protección de los soportes de información [mp.si]» y Limpieza de documentos del capítulo de «Protección de la información [mp.info]».

VII. Asignación de metadatos

VII.1 Las organizaciones garantizarán la disponibilidad e integridad de los metadatos de sus documentos electrónicos, manteniendo de manera permanente las relaciones entre cada documento y sus metadatos.

VII.2 La implementación de los metadatos de gestión de documentos electrónicos para su tratamiento y gestión a nivel interno será diseñada por cada organización en base a sus necesidades, criterios y normativa específica.

VII.3 Los metadatos de gestión de documentos electrónicos se articularán en esquemas de metadatos que responderán a las particularidades y necesidades específicas de gestión de cada organización.

VII.4 El Esquema de Metadatos para la Gestión del Documento Electrónico (e-EMGDE), disponible en el Centro de Interoperabilidad Semántica, que incluye los metadatos mínimos obligatorios, definidos en las Normas Técnicas de Interoperabilidad de Documento electrónico y Expediente electrónico, así como otros metadatos complementarios pertinentes en una política de gestión y conservación de documentos electrónicos, podrá ser utilizado como referencia para la adecuación a los requisitos de interoperabilidad en materia de gestión documental.

VIII. Documentación

Cada organización elaborará y mantendrá actualizados y documentados los procedimientos de gestión de documentos a seguir en los distintos procesos de gestión documental.

IX. Formación

IX.1 El personal de las organizaciones recibirá la formación específica y adecuada a su rol necesaria para la gestión y conservación de documentos y expedientes electrónicos.

IX.2 Las organizaciones exigirán, de manera objetiva y no discriminatoria, que aquellos que les presten servicios relacionados con la gestión y conservación documental cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados.

X. Supervisión y auditoría

X.1 Los procedimientos y acciones seguidos en los distintos procesos de gestión documental generarán registros con las evidencias de la correcta aplicación de dichos procedimientos atendiendo a las necesidades de cada documento y organización.

X.2 Las organizaciones realizarán evaluaciones o auditorías periódicas, convenientemente documentadas, que garanticen la adecuación de la política de gestión documental y que los procesos de gestión de documentos electrónicos se realizan conforme a lo establecido en la política.

X.3 Los resultados de dichas evaluaciones serán considerados para la actualización de la política, programa de tratamiento y procesos de gestión de documentos electrónicos.

XI. Actualización

La política de gestión de documentos electrónicos, el programa de tratamiento y los procesos de gestión documental serán convenientemente actualizados con el fin de garantizar su adecuación permanente a las necesidades reales de gestión de documentos electrónicos y normativa aplicable.

§ 35

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de requisitos de conexión a la red de comunicaciones de las Administraciones Públicas españolas

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13173

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas se desarrolla bajo lo establecido en el artículo 43 de la Ley 11/2007, de 22 de junio, y artículo 13 del Real Decreto 4/2010, de 8 de enero, para posibilitar la interconexión de las redes de las Administraciones públicas y permitir el intercambio de información entre las mismas, así como la interconexión con las redes de las Instituciones de la Unión Europea y de otros Estados Miembros.

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas establece las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla, accederá a la Red SARA, y describe los roles y responsabilidades de los agentes que se conectan a la Red SARA así como los requisitos para la conexión, acceso y uso de los servicios que se prestan a través de aquélla.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE REQUISITOS DE CONEXIÓN A LA RED DE COMUNICACIONES DE LAS ADMINISTRACIONES PÚBLICAS ESPAÑOLAS

I. Consideraciones generales

I.1 *Objeto*.–La Norma Técnica de Interoperabilidad de Requisitos de conexión a la Red de comunicaciones de las Administraciones públicas españolas tiene por objeto establecer las condiciones en las que cualquier órgano de una Administración, o Entidad de Derecho Público vinculada o dependiente de aquélla (en adelante, organización), accederá a la Red SARA.

I.2 *Ámbito de aplicación*.–El contenido de esta norma será de aplicación en la conexión a la Red SARA en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

II. Agentes y conexión a la Red SARA

II.1 *Conexión a la Red SARA.*

1. El acceso a la Red SARA se realizará a través de lo que se denomina Punto de Presencia (PdP) entendido como cualquier sede en la que existe una conexión directa a la Red SARA, sin presencia de ninguna organización intermedia.

2. Entre los PdPs de la Red SARA podrán distinguirse los siguientes tipos:

a) Proveedores de Acceso a la Red SARA (PAS).

b) Centros de Proceso de Datos (CPD) de SARA.

c) Red sTESTA (secure Trans-European Services for Telematics between Administrations).

d) Centros externos de monitorización.

e) Prestadores de servicios de certificación.

f) Otros: como son las Ventanillas Únicas Empresariales.

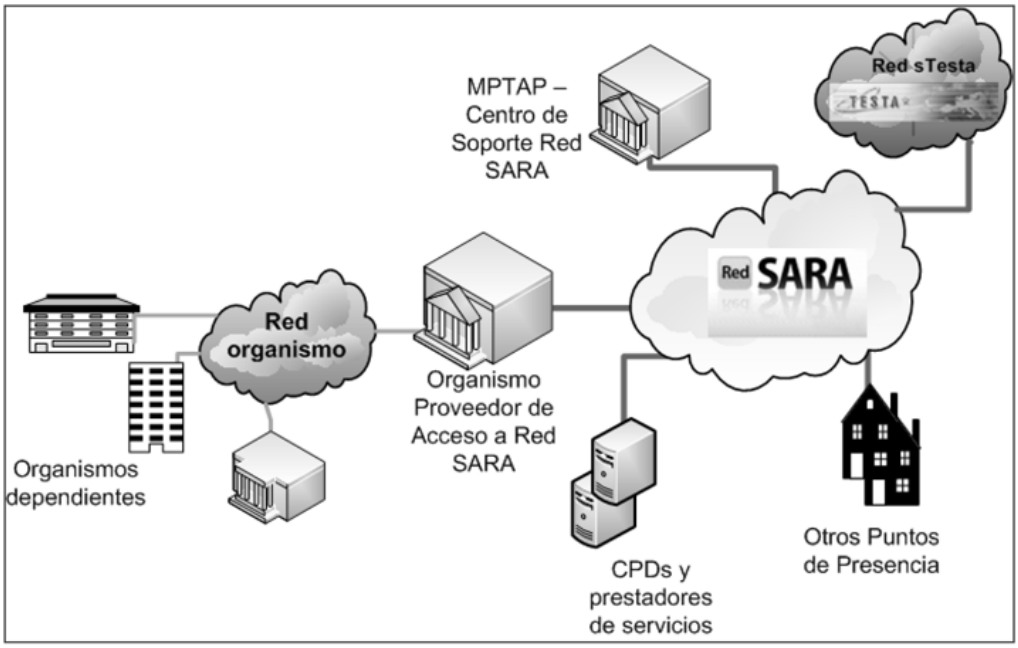


Figura 1. Puntos de Presencia y esquema de conexión a Red SARA

3. Con independencia de casos especiales de PdPs, en la conexión de cualquier organización a la Red SARA será necesaria la intervención del Ministerio de Política Territorial y Administración Pública (en adelante, MPTAP), un proveedor de acceso y la propia organización que desea conectarse, que actuará como usuario final.

II.2 *MPTAP-Centro de Soporte de la Red SARA.*–Las funcionalidades prestadas por el Centro de Soporte de la Red SARA del MPTAP se podrán consultar en el portal web www.redsara.es, accesible desde la Red SARA.

II.3 *Proveedores de Acceso a la Red SARA (PAS).*

1. La conexión directa a la Red SARA se proporcionará a través de un Área de Conexión (AC) que se ubicará en las dependencias de la Administración pública correspondiente convirtiéndose ésta en Proveedor de Acceso a la Red SARA (PAS) para sus Unidades, Organismos y Entidades de Derecho Público dependientes y, en el caso de las Comunidades Autónomas, también para las Administraciones Locales de su ámbito territorial.

2. Las organizaciones que no están adscritas a ningún organismo superior: Ministerios, Comunidades y ciudades con Estatuto de Autonomía y Órganos constitucionales, funcionarán como PAS a excepción de las Administraciones Locales que quedarán asignadas al PAS de la Comunidad Autónoma correspondiente.

3. Otros organismos públicos podrán asumir las funciones de PAS siempre que el MPTAP así lo establezca atendiendo a la singularidad del organismo o a la prestación, por parte de aquél, de servicios considerados singulares.

4. El establecimiento de un nuevo PAS, a solicitud del interesado, corresponderá al MPTAP a través del Centro de Soporte de la Red SARA.

II.4 *Órganos usuarios finales.*

1. Todo órgano usuario final de la Red SARA accederá a ésta a través de una organización que ejercerá las funciones de PAS.

2. Las características y dispositivos de la conexión de los órganos finales con el PAS correspondiente dependerán de las condiciones y mecanismos que disponga el propio PAS.

3. La solicitud de conexión de los órganos finales se dirigirá directamente al PAS del que dependen y será comunicada al Centro de Soporte de la Red SARA.

4. El listado completo de PAS estará disponible en el portal web www.redsara.es, accesible desde la Red SARA.

III. Requisitos técnicos para la conexión del PAS

III.1 *Esquema del Área de Conexión (AC).*

1. El AC de un PAS funcionará como punto único de conexión entre la red de la Administración pública correspondiente y sus organizaciones dependientes o asignadas al PAS, a las redes de otras administraciones y Entidades públicas conectadas a la Red SARA, así como a la Red sTESTA de la Comisión Europea.

2. La estructura del AC responderá al esquema de una zona desmilitarizada (DMZ) delimitada por un subsistema de seguridad externo, que conectará con el resto de la Red SARA, y un subsistema de seguridad interno hacia el interior de la organización.

3. Los elementos del AC, además de proporcionar seguridad perimetral, albergarán los servicios telemáticos básicos prestados por la Red SARA: DNS, SMTP, NTP, Proxy y Proxy inverso.

4. El subsistema de seguridad externo será el encargado de establecer una red privada virtual (VPN) hacia el resto de sedes de la Red SARA, con lo que todas las comunicaciones, a través del operador de servicios de telecomunicaciones, estarán cifradas mediante túneles.

5. En la zona intermedia, DMZ, será posible conectar cualquier equipo que la organización considere conveniente utilizar para la comunicación con el resto de organizaciones que componen la Red. Para no vulnerar la seguridad global de la Red, el Centro de Soporte de la Red SARA del MPTAP determinará las condiciones en que dichos elementos adicionales deberán integrarse en el AC.

6. Un esquema muy simplificado de un AC es el siguiente:

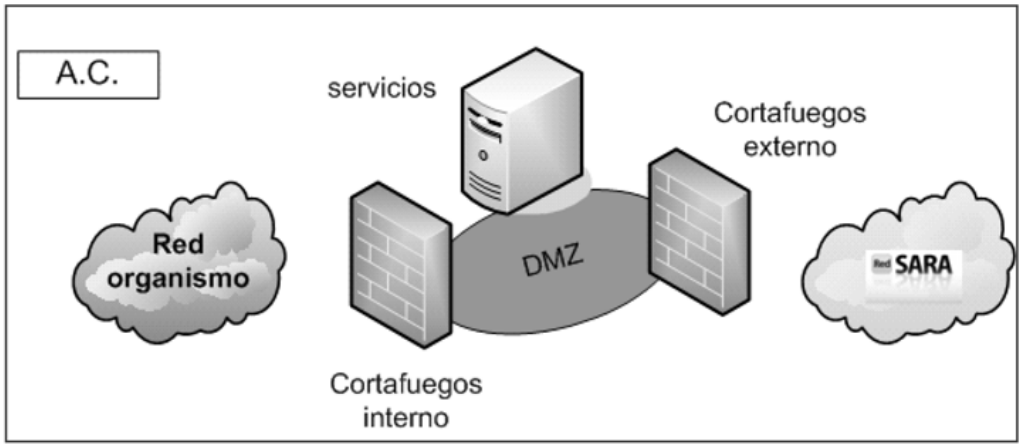


Figura 2. Esquema lógico de un Área de Conexión (AC)

III.2 *Administración de la conexión.*–El MPTAP administrará la conexión a la Red SARA y aplicará las políticas necesarias para el aseguramiento de la interoperabilidad y el nivel de seguridad correspondiente.

III.3 *Plan de direccionamiento.*

1. Las organizaciones que se conecten a la Red SARA aplicarán el Plan de direccionamiento e Interconexión de Redes en la Administración establecido por la Dirección General para el Impulso de la Administración Electrónica (DGIAE) disponible en http://administracionelectronica.gob.es/ según lo dispuesto en artículo 14 del Real Decreto 4/2010, de 8 de enero.

2. Todas las partes pondrán todos los medios a su alcance para adaptarse a los correspondientes planes de direccionamiento, de tal manera que un determinado rango o espacio de direcciones IP será reservado para preservar la compatibilidad e interoperabilidad.

III.4 *Dotación de elementos de conectividad.*–El MPTAP adquirirá, instalará, administrará, configurará y mantendrá los elementos de conectividad de cada PAS.

III.5 *Garantías de acondicionamiento físico.*–El acondicionamiento físico de las instalaciones del PAS cumplirá lo establecido a tal efecto en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica de manera que se asegure la continuidad del servicio.

III.6 *Servicios de soporte y gestión de incidentes.*

1. El soporte y la gestión de incidentes de la Red SARA se prestarán de manera conjunta entre el MPTAP y los PAS, a través de sus correspondientes equipos dedicados a estos servicios.

2. Para facilitar la actuación conjunta entre el MPTAP y los PAS, cada organización proporcionará los siguientes datos de sus servicios de soporte y de gestión de incidentes:

a) Identificación.
b) Responsable de la unidad.
c) Responsable técnico.
d) Horario de servicio.
e) Localización.
f) Horario y datos de contacto para incidentes.
g) Observaciones.

3. Los datos identificativos y de contacto de los servicios de soporte y de gestión de incidentes de cada organización serán convenientemente actualizados y distribuidos entre todos los agentes de manera que se asegure la disponibilidad de la información de contacto para actuar ante cualquier incidente. Su consulta estará disponible a través del portal web www.redsara.es, accesible desde la Red SARA.

IV. Acceso y utilización de servicios

IV.1 *Acceso a los servicios.*

1. Cualquier organización con conexión a la Red SARA, podrá solicitar la utilización de cualquiera de los servicios que se presten a través de ésta.

2. El catálogo de servicios disponibles en la Red SARA estará disponible en el portal web www.redsara.es, accesible desde la Red SARA.

IV.2 *Mantenimiento del catálogo de servicios.*

1. El catálogo de servicios será mantenido y actualizado por el MPTAP y el PAS a través del cual se presta cada servicio.

2. Todos los servicios que se publiquen en la Red SARA, a través de un PAS, serán comunicados al Centro de Soporte de la Red SARA con el fin de mantener el catálogo de servicios correctamente actualizado.

3. El catálogo de servicios facilitará la elaboración de estadísticas y cuadros de mando que el MPTAP podrá publicar en el portal web www.redsara.es y poner a disposición de todos los implicados.

IV.3 *Condiciones de utilización de los servicios.*

1. Para los servicios verticales o de negocio, así como para los servicios comunes de administración electrónica, con independencia de condiciones particulares que pudiese establecer el prestador del servicio, las condiciones de utilización serán

a) Acuerdo previo entre la Administración pública que presta el servicio y la beneficiaria.
b) Comunicación al Centro de Soporte de la Red SARA del MPTAP.
c) Si procede, condiciones de la plataforma de intermediación de datos que intervenga en el servicio. En caso de uso de la Plataforma de intermediación del MPTAP, se atenderá a lo establecido en la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos.

2. La solicitud de alta de un nuevo servicio y las comunicaciones al Centro de Soporte de la Red SARA se realizarán a través de los medios dispuestos para tal fin en el portal web www.redsara.es, donde figurarán, al menos, los siguientes datos:

a) Datos del solicitante.
b) Datos generales del servicio.

i. Nombre del servicio o aplicación.
ii. Nivel de criticidad.
iii. Horario de disponibilidad.
iv. Destinatarios del servicio.

c) Datos del soporte técnico para el contacto con dicho servicio.
d) Datos técnicos de acceso y uso del servicio.

V. Agentes y roles

V.1 *Ministerio de Política Territorial y Administración Pública.*–El MPTAP:

a) Instalará, administrará y mantendrá una conexión de capacidad suficiente y alta disponibilidad ubicada en las dependencias que la Administración pública determine y que mejor permita la conexión con su correspondiente red para constituirse como PAS.

b) Proporcionará a los responsables del PAS la documentación técnica correspondiente a la arquitectura y configuración de los sistemas que componen el AC.

c) Mantendrá un servicio de soporte 24x7 para garantizar la continuidad del servicio en el AC y la red troncal que sirva para realizar la gestión de incidentes y problemas, cuando le corresponda, así como la gestión de la resolución cuando intervengan agentes externos (fabricantes, operadores u otros organismos con acceso al sistema), consultas técnicas relacionadas con el servicio o peticiones de nuevos accesos.

d) Gestionará el portal web www.redsara.es, como espacio para facilitar información general sobre la Red SARA así como información específica para los responsables técnicos del PAS respecto del servicio proporcionado, notificación de incidencias, paradas programadas, publicación de nuevos servicios y otras informaciones de interés.

e) Adoptará las medidas de seguridad necesarias para proteger debidamente la información transmitida, mediante el cifrado de las comunicaciones y la detección temprana de incidentes en colaboración con el CCN-CERT.

V.2 *Proveedores de acceso a la Red SARA.*–Cualquier Administración pública que funcione como PAS:

a) Realizará las labores de conectividad y despliegue pertinentes para poder acceder desde sus propias dependencias o instalaciones a la Red SARA a través del AC.

b) Gestionará y mantendrá los elementos activos que conectan su red corporativa a la Red SARA.

c) Garantizará condiciones adecuadas en la ubicación del AC (condiciones medioambientales, suministro eléctrico, cableado, etc.) con el fin de asegurar la continuidad del servicio.

d) Mantendrá un servicio de soporte, a ser posible 24x7, para garantizar la continuidad del servicio en su función como PAS. Para ello se facilitarán al MPTAP los contactos, tanto de los responsables del PAS como los del Centro de Soporte, Centro de Atención al Usuario o equivalente.

e) Colaborará con el MPTAP en la gestión de incidentes y problemas, incluso si ello lleva consigo pequeñas comprobaciones o actuaciones en el AC, dirigidas desde el Centro de Soporte de la Red SARA, con el fin de reducir los tiempos de resolución de las incidencias que pudieran ocurrir.

f) Facilitará, promoverá y sostendrá el acceso a la Red SARA a sus Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de Comunidades Autónomas, a las Administraciones Locales de su ámbito territorial, con la tecnología, mecanismos y procedimientos que éstos acuerden, garantizando la continuidad del servicio y las condiciones adecuadas de seguridad en la parte que le corresponde.

g) Colaborará con el MPTAP en el mantenimiento del catálogo de servicios y conexiones.

V.3 *Órganos usuarios finales.*–Los Organismos y Entidades de Derecho Público dependientes y adicionalmente, en el caso de Comunidades Autónomas, las Administraciones Locales de su ámbito territorial, que disfruten del acceso a la Red SARA a través del PAS correspondiente, aplicarán:

a) Condiciones particulares del PAS del que dependen.
b) Condiciones particulares de servicios horizontales y verticales que utilizan a través de la Red SARA.

V.4 *Publicidad de referencias.*

1. El MPTAP podrá hacer pública, en cualquier lista de referencia o en cualquier boletín de prensa publicado y sin autorización previa, la relación de organismos usuarios de la Red SARA.
2. Las Administraciones públicas podrán referenciar la utilización de la Red SARA sin autorización previa por parte del MPTAP.

§ 36

Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos

Ministerio de Política Territorial y Administración Pública
«BOE» núm. 182, de 30 de julio de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-13172

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas Normas Técnicas de Interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio.

Dentro de este conjunto de Normas Técnicas de Interoperabilidad, las normas relativas al documento electrónico, al expediente electrónico, a la digitalización de documentos en soporte papel, a los procedimientos de copiado auténtico y conversión y a la política de gestión de documentos electrónicos responden a lo previsto en el citado Real Decreto 4/2010, de 8 de enero, sobre interoperabilidad, recuperación y conservación del documento electrónico, a la luz de la necesidad de garantizar todos estos aspectos para el documento electrónico a lo largo del tiempo.

En particular, la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos establece las reglas para la generación y expedición de copias electrónicas auténticas, copias papel auténticas de documentos públicos administrativos electrónicos y para la conversión de formato de documentos electrónicos por parte de las Administraciones públicas; para los aspectos relativos a la gestión de los documentos resultantes del proceso de copiado auténtico o conversión, se remite a la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE PROCEDIMIENTOS DE COPIADO AUTÉNTICO Y CONVERSIÓN ENTRE DOCUMENTOS ELECTRÓNICOS

I. Objeto

La Norma Técnica de Interoperabilidad de Procedimientos de copiado auténtico y conversión entre documentos electrónicos tiene por objeto establecer las reglas para la generación de copias electrónicas auténticas, copias papel auténticas de documentos públicos administrativos electrónicos y para la conversión de formato de documentos electrónicos.

II. Ámbito de aplicación

Esta norma será de aplicación en los procedimientos de copiado auténtico y conversión entre documentos electrónicos en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

III. Características generales de las copias electrónicas auténticas

III.1 Las copias electrónicas generadas que, por ser idénticas al documento electrónico original no comportan cambio de formato ni de contenido, tendrán la eficacia jurídica de documento electrónico original.

III.2 Las copias auténticas se expedirán a partir de documentos con calidad de original o copia auténtica.

III.3 Las copias electrónicas auténticas serán nuevos documentos electrónicos que incluirán total o parcialmente el contenido del documento sobre el que se expiden y que

cumplirán con lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico.

III.4 El valor de cada uno de los metadatos mínimos obligatorios del documento electrónico copia será asignado en función de las características propias de cada metadato y de las propiedades específicas del documento bajo la responsabilidad del órgano u Organismo que lo expide.

III.5 La relación entre la copia electrónica auténtica y el documento origen se reflejará en los metadatos del documento electrónico copia a través del metadato «Identificador del documento origen» que tomará el valor del identificador de aquél.

III.6 Las copias electrónicas auténticas serán firmadas mediante alguno de los sistemas de firma previstos en los artículos 18 ó 19 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

IV. Copia electrónica auténtica con cambio de formato

Las copias electrónicas auténticas con cambio de formato:

1. Se obtendrán de la aplicación de una conversión entre documentos electrónicos que se realizará según lo establecido en el apartado VIII de esta norma.

2. Tendrán asignado el valor «Copia electrónica auténtica con cambio de formato» en el metadato mínimo obligatorio «Estado de elaboración».

V. Copia electrónica auténtica de documentos papel

Las copias electrónicas auténticas de documentos en soporte papel o en otro soporte no electrónico susceptible de digitalización a través de medios fotoeléctricos:

1. Se obtendrán de la digitalización del documento origen según lo establecido en la Norma Técnica de Interoperabilidad de Digitalización de documentos.

2. Tendrán asignado el valor «Copia electrónica auténtica de documento papel» al metadato mínimo obligatorio «Estado de elaboración».

VI. Copia electrónica parcial auténtica

Las copias electrónicas parciales auténticas:

1. Se obtendrán mediante extractos del contenido del documento origen que corresponda o a través de la utilización de otros métodos electrónicos que permitan mantener la confidencialidad de aquellos datos que no afecten al interesado.

2. Tendrán asignado el valor «Copia electrónica parcial auténtica» en el metadato mínimo obligatorio «Estado de elaboración».

VII. Copia papel auténtica de documentos públicos administrativos electrónicos

Para la obtención de copias auténticas en soporte papel de documentos públicos administrativos electrónicos se atenderá a lo previsto en la normativa aplicable y a lo establecido sobre el acceso a documentos electrónicos en la Norma Técnica de Interoperabilidad de Documento electrónico para la verificación de su autenticidad.

VIII. Conversión entre documentos electrónicos

VIII.1 La conversión entre documentos electrónicos supondrá la generación de un nuevo documento electrónico con diferente formato o versión a la del documento origen que cumplirá con lo establecido en la Norma Técnica de Interoperabilidad de Documento electrónico.

VIII.2 La conversión entre documentos electrónicos se realizará atendiendo a:

a) La aplicación de procedimientos de conversión establecidos en un marco de gestión documental definido según la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos.

b) La conservación del contenido, contexto y estructura del documento origen e identificación de componentes que requieran, dada su naturaleza, un tratamiento específico en la conversión.

c) El formato del nuevo documento convertido será seleccionado de entre los establecidos en la Norma Técnica de Interoperabilidad de Catálogo de estándares y permitirá la reproducción de la información contenida en el documento original minimizando el riesgo de pérdida de información.

VIII.3 En el caso de que el documento resultado de la conversión deba ser conformado como copia auténtica, se contemplarán, adicionalmente, los requisitos establecidos en los apartados III y IV de esta norma.

§ 37

Resolución de 22 de julio de 2021, de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por la que se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las entidades registrales

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 190, de 10 de agosto de 2021
Última modificación: sin modificaciones
Referencia: BOE-A-2021-13749

El Esquema Nacional de Interoperabilidad (ENI) se establece en el artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que sustituye al apartado 1 del artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia, en el marco, entre otras normas, de la Ley 39/2015 de Procedimiento Administrativo Común de las Administraciones Públicas.

El Esquema Nacional de Interoperabilidad se establece en el apartado 1 del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Su finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permitan el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica establece, en su disposición adicional primera, el desarrollo de la serie de Normas Técnicas de Interoperabilidad que son de obligado cumplimiento por parte de las Administraciones públicas.

Las Normas Técnicas de Interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano.

En particular, la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las entidades registrales se aprobó mediante Resolución de 19

de julio de 2011 (BOE de 30 de julio), de la Secretaría de Estado para la Función Pública, para responder a lo recogido en el artículo 24.4 de la Ley 11/2007, de 22 de junio, sobre garantía de interconexión de todas oficinas de registro y posibilitar el acceso por medios electrónicos a los asientos registrales y a las copias electrónicas de los documentos presentados.

Posteriormente, la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y las previsiones recogidas en su artículo 16.4, que establece que los registros electrónicos de todas y cada una de las Administraciones, deberán ser plenamente interoperables, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de los asientos registrales y de los documentos que se presenten en cualquiera de los registros, hacen necesario la actualización de esta Norma Técnica de Interoperabilidad.

Así, la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales, que sustituye a la anterior, normaliza los intercambios registrales entre las oficinas de registro para garantizar su interoperabilidad y, como novedad, permite la adecuación de los intercambios a las nuevas necesidades de las oficinas de registro y favorece el avance hacia una tramitación automatizada de la documentación intercambiada.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por el Comité de Dirección de Tecnologías de la Información y Comunicaciones y por la Comisión Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero,

Esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (SICRES4), que sustituye a la anterior Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (SICRES3) de 2011, y cuyo texto se incluye a continuación.

Segundo.

La Norma Técnica de Interoperabilidad de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales (SICRES4) que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Desde su publicación en el «Boletín Oficial del Estado» se dispondrá de un año para la adaptación de la anterior Norma Técnica de Interoperabilidad. Durante ese período, ambas versiones estarán vigentes.

NORMA TÉCNICA DE INTEROPERABILIDAD DE MODELO DE DATOS PARA EL INTERCAMBIO DE ASIENTOS ENTRE LAS ENTIDADES REGISTRALES

I. SICRES: Sistema de Información Común de Registros de Entrada y Salida

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (en adelante, Ley 30/1992), estableció por primera vez la posibilidad de que las Administraciones públicas utilizaran medios electrónicos y telemáticos en su relación con el ciudadano. Dentro de este ámbito se incluía inicialmente la integración informática de los registros generales con los restantes registros administrativos (artículo 38.3 de la Ley 30/1992, de 26 de noviembre).

Posteriormente, el legislador amplió las potestades de las Administraciones en este ámbito a través de la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, que venía a añadir un nuevo apartado al ante dicho artículo 38 por el que

se reconocía «la posibilidad de crear registros telemáticos para la recepción o salida de solicitudes, escritos y comunicaciones que se transmitan por medios telemáticos».

Siguiendo el espíritu de la Ley 30/1992, de 26 de noviembre, el Consejo Superior de Informática (en adelante, CSI), en aquel momento Consejo Superior de Administración Electrónica según el Real decreto 589/2005, (en adelante, CSAE), definió en 1995 por primera vez, el estándar SICRES versión 1.0 (Sistemas de Información Común de Registros de Entrada y Salida) por el que se fijaban los criterios que debían cumplir todos los sistemas de Registro que se implantaran en la Administración, versión que fue actualizada en 1999 por el CSI a través de la norma SICRES versión 2.0.

En definitiva, con la definición de SICRES se perseguía lograr una tramitación más eficaz de los expedientes a través de un Registro Central interconectado con las distintas oficinas registrales y garantizar los derechos que la citada Ley 30/1992 reconocía.

Posteriormente, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicio Públicos, volvió a ratificar la regulación de los registros electrónicos administrativos y la interconexión de estos. Así, el artículo 24 de esta ley, estableció que las Administraciones Públicas crearían registros electrónicos para la recepción y remisión de solicitudes, escritos y comunicaciones.

En 2010, se aprobó el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, el cual es de aplicación a todas las Administraciones Públicas. En el artículo 25 de este Real Decreto, se establece que los registros electrónicos deben regirse por lo establecido en el Esquema Nacional de Interoperabilidad, y por tanto también por las Normas Técnicas de Interoperabilidad aprobadas a raíz de este.

Así, se aprobó en 2010, con aplicación a todas las Administraciones Públicas, la Norma Técnica de Interoperabilidad de Modelo de Datos para el Intercambio de asientos entre las Entidades Registrales, la cual aprobaba la versión 3 de la norma SICRES. Esta norma SICRES3.0 presentaba las principales diferencias con respecto a sus predecesoras:

i. Orientación a arquitectura de intermediación.
ii. Incorporación de ficheros adjuntos a los intercambios.
iii. Mejora en los mecanismos de control del intercambio.

II. Objetivo y alcance de esta Norma Técnica de Interoperabilidad

El objetivo de la Norma Técnica de Interoperabilidad (en adelante, NTI) de Modelo de Datos para el intercambio de asientos entre las Entidades Registrales es definir las condiciones y características para la interconexión de registros de las Administraciones públicas, y, por tanto, el intercambio de información entre estas.

Para ello, esta NTI contiene la especificación SICRES 4.0, evolución de su antecesora SICRES 3.0,

Su contenido abarca los siguientes puntos:

i. Definición y características principales de SICRES 4.0
ii. Esquema de datos y formatos para los ficheros intercambiados.
iii. Mecanismos de control y gestión de errores a aplicar en el proceso.
iv. Prestaciones de alto nivel a garantizar por el sistema de intercambio utilizado.

III. Ámbito de aplicación y destinatarios

El contenido de esta NTI es de aplicación para todos los órganos de la Administración pública o Entidades de derecho Público vinculadas o dependientes de aquélla (en adelante, organizaciones) que participan en el intercambio de asientos registrales, ya sea para la prestación de servicios directos a los ciudadanos, como de cara al intercambio de información con otros órganos.

Dentro del ámbito de aplicación definido, los destinatarios del contenido de esta norma son los siguientes:

i. Responsables de sedes electrónicas y, por tanto, de garantizar los requisitos de interoperabilidad de las mismas y, concretamente, de sus registros electrónicos.

ii. Responsables y administradores de aplicaciones, redes y servicios corporativos de cualquier órgano.

IV. Modelo de datos para el intercambio de asientos entre Entidades Registrales

IV.1 Definición y características generales de SICRES 4.0.

SICRES 4.0 constituye el modelo de datos para el intercambio de asientos entre Entidades Registrales. Esta versión de SICRES, alineada con la filosofía de sus predecesoras, tiene como finalidad contribuir a garantizar la interconexión entre organizaciones, permitiendo así, un servicio de mayor calidad a los ciudadanos tal y como marca la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Las principales características de SICRES 4.0 que la diferencian de sus versiones anteriores son:

i. Reordenación, actualización e incorporación de campos. El modelo de intercambio SICRES 4.0 agrupa y reordena los campos de los distintos segmentos para dotarlos de mayor contenido semántico y facilitar su interpretación. Asimismo, se eliminan o actualizan campos obsoletos y se incorporan nuevos campos.

ii. Referenciación de documentos electrónicos. Se sustituye el intercambio de los ficheros de los documentos electrónicos objeto de registro e intercambio, por el intercambio de referencias a tales documentos electrónicos. De este modo, se optimiza el funcionamiento de la Plataforma de Intercambio y se superan limitaciones de la misma.

iii. Metadatado para automatización del tratamiento de los asientos registrales y sus documentos anexos. Se incorporan en el intercambio registral nuevos metadatos destinados a facilitar la automatización del tratamiento de los asientos y los documentos electrónicos. Asimismo, se incorpora la posibilidad de intercambiar otros metadatos no definidos a priori, bien sea para cubrir necesidades futuras, o bien sea para cubrir necesidades particulares de cada organismo.

Durante el período de transición de las aplicaciones de registro de SICRES 3.0 a SICRES 4.0 se garantizará la interoperabilidad entre ambas normas. La plataforma de intercambio de asientos registrales SIR se encargará de garantizar la compatibilidad y la comunicación entre aplicaciones de registro que utilicen diferentes versiones de la norma.

El modelo conceptual de espacio de intercambio bajo SICRES 4.0 aparece en la siguiente figura:

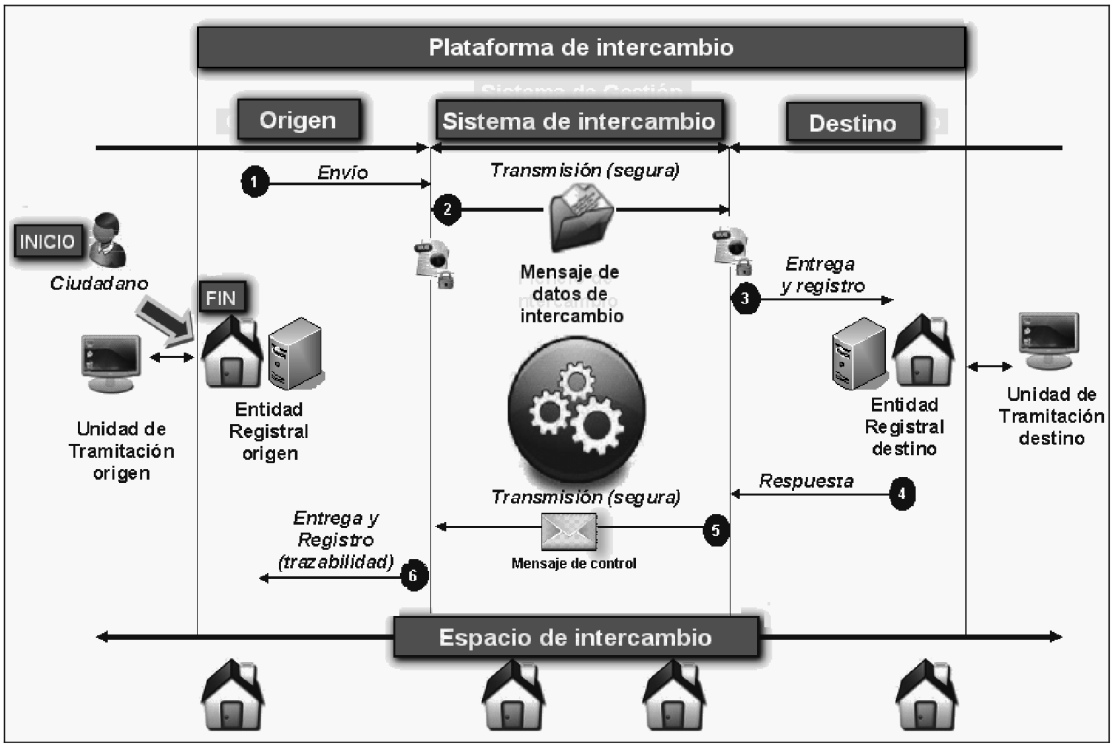


Figura 1. Esquema del modelo de intercambio de SICRES 4.0

Según este esquema, el espacio de intercambio engloba todo el proceso de intercambio desde la Unidad de Tramitación Origen hasta la Unidad Tramitación Destino proporcionando un contexto único a cada uno de los intercambios. Dentro de este espacio, destacan los siguientes elementos:

Unidades de Tramitación de Origen y Destino: Entidades, o unidades pertenecientes a dichas entidades, responsables de la tramitación de los documentos registrados. La identificación de ambas Unidades debe ser única a través de Directorios unificados, como se indica en el apartado VI.4 de esta norma.

Entidad Registral de Origen y Destino. Entidades, o unidades pertenecientes a dichas entidades, que, bien sea por medio del personal al servicio del mismo, o bien sea por medio de actuación automatizada, se encarga tanto de inscribir los asientos de entrada y salida en el Registro Electrónico de la Administración u Organismo, como de llevar a cabo el proceso de intercambio registral, responsabilizándose del envío y recepción de Mensajes de Datos de Intercambio y Mensajes de Control, desde el punto de vista técnico y de comunicación, pero sin implicación en la tramitación de los documentos. La identificación de ambas Entidades Registrales debe ser única a través de Directorios unificados, como se indica en el apartado VI.4 de esta norma.

Mensaje de datos de intercambio. Es creado y emitido por la Entidad Registral de Origen y alberga, además de campos para el control e identificación, la información del asiento registral y los documentos correspondientes adjuntos. Su estructura y formato se definen en el apartado IV.2 de esta norma.

Mensajes de control. Son emitidos por la Entidad Registral destino o por el propio sistema de intercambio y proporcionan información de estado para la gestión de la operación de intercambio. Su estructura y formato se definen en el apartado IV.3 de esta norma.

Sistema de intercambio. Proporciona la gestión del intercambio y la comunicación directa con las Entidades Registrales Origen y Destino. Sus funciones y requisitos técnicos deben cumplir lo establecido en el apartado VI de esta norma.

Plataforma de intercambio. Comprende el Sistema de intercambio y las Entidades Registrales de Origen y de Destino.

El proceso de intercambio inicia y finaliza en la Entidad Registral de Origen, punto de contacto con el ciudadano o Unidad de Tramitación que origina la creación del asiento registral.

El inicio viene marcado por la generación del mensaje de datos de intercambio en la Entidad Registral Origen conteniendo la información del asiento. A través del sistema de intercambio, este mensaje es recibido en la Entidad Registral destino, que, si procede, confirma la recepción correcta al Origen a través del mensaje de control correspondiente.

Los intercambios disfrutan de un contexto único dentro del espacio SICRES mediante la asignación de un identificador del intercambio único a cada proceso de transacción que es generado por la aplicación de registro de la Entidad Registral de Origen y acompaña tanto al mensaje de datos de intercambio como a los mensajes de control relacionados. La generación del identificador del intercambio se detalla en el apartado V.1 de esta NTI.

IV.2 Estructura y contenido del mensaje de datos de intercambio.

El mensaje de datos de intercambio de SICRES4.0 es el mensaje que alberga la información objeto del intercambio. Su codificación se especifica con un ejemplo de implementación del modelo en XML en el Anexo 2 de esta norma.

Este mensaje está compuesto por los 7 segmentos que aparecen en la figura y cuya descripción funcional se desarrolla a continuación.

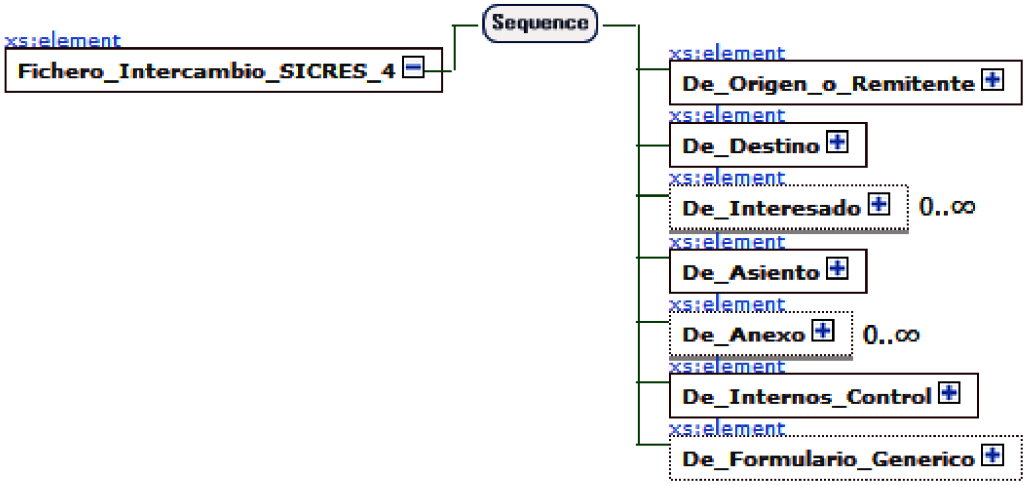


Figura 2. Estructura del fichero de intercambio de SICRES 4.0

Segmento de Origen (o Remitente).

Segmento de Origen (o Remitente)				☑ Obligatorio ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Código Entidad Registral de Origen.	Alfanumérico.	21	Obligatorio.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4.
Decodificación de Entidad Registral de Origen.	Alfanumérico.	120	Opcional.	Descripción de la Entidad Registral de Origen.
Código de la Unidad de Tramitación de Origen.	Alfanumérico.	21	Condicional.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4. La cumplimentación de este campo es obligatoria cuando el emisor del registro es un órgano u organismo perteneciente o dependiente de una Administración Pública.
Decodificación de la Unidad de Tramitación de Origen.	Alfanumérico.	120	Opcional.	Descripción de la Unidad de Tramitación Origen.

Tabla 1. Datos de Origen (o Remitente)

La cumplimentación de la Unidad de Tramitación de Origen será obligatoria cuando el emisor del registro sea un órgano u organismo perteneciente o dependiente de una Administración Pública, como se indica en el comentario del campo.

Sin embargo, no será obligatoria la cumplimentación de este campo en los reenvíos o rechazos que se realicen de registros emitidos por Administraciones Públicas. Asimismo, tampoco será obligatoria la cumplimentación, en envíos registrales que se traten de rectificaciones de intercambios previos. Es decir, en envíos registrales que realicen órganos y organismos de las Administraciones Públicas como consecuencia de haber confirmado por error un registro que habían recibido.

B) Segmento de destino.

Segmento de destino (o destinatario)				**☑ Obligatorio ☑ Único**
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Código Entidad Registral de Destino.	Alfanumérico.	21	Obligatorio.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4.
Decodificación Entidad Registral de Destino.	Alfanumérico.	120	Opcional.	Descripción de Entidad Registral de destino.
Código de la Unidad de Tramitación de Destino.	Alfanumérico.	21	Condicional.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4. La cumplimentación de este campo es obligatoria cuando el destinatario del registro es un órgano u organismo perteneciente o dependiente de una Administración Pública.
Decodificación de la Unidad de Tramitación de Destino.	Alfanumérico.	120	Opcional.	Descripción de la Unidad de Tramitación de destino.

Tabla 2. Datos de destino

C) Segmento de Interesado.

Este segmento comprende los datos que identifican al Interesado y su Representante en la entidad mensaje de datos de intercambio. Este segmento se puede declarar de forma múltiple. Su condicionalidad se define en los comentarios de los campos «Datos del Interesado» y «Datos del Representante».

Segmento de Interesado				**☑ Condicional ☑ Múltiple**
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Datos del Interesado.	Tipo complejo. (Datos Persona).		Condicional.	Este campo comprende todos los datos personales del interesado; tanto datos de identidad, como datos de contacto e información relativa a los canales de notificaciones. Este campo deberá cumplimentarse siempre que el intercambio se realice en el marco de un procedimiento administrativo en el cual existe y se conoce el interesado. En cualquier caso, será obligatorio siempre que se trate de un registro de entrada. También deberá tenerse en cuenta que será obligatorio siempre que se indique Representante. Estos campos deberán cumplimentarse con independencia de que la información sea redundante con la ya indicada en los Segmentos de Origen o Destino. Se compone de los siguientes campos: *Datos de identificación*, *Datos de contacto*, *Receptor notificaciones* y *Canales de notificación.*
Datos del Representante.	Tipo complejo. (Datos Persona).		Condicional.	Este campo comprende todos los datos personales del representante; tanto datos de identidad, como datos de contacto e información relativa a los canales de notificación. Este campo no podrá cumplimentarse si no se ha cumplimentado el campo «Datos del Interesado». Se compone de los siguientes campos: *Datos de identificación*, *Datos de contacto*, *Receptor notificaciones* y *Canales de notificación.*
Observaciones.	Alfanumérico.	160	Opcional.	Observaciones del Interesado y/o del Representante.
Tipo complejo: Datos Persona.				
Datos de identificación.	Tipo complejo. (Datos Identificación).		Obligatorio.	Se compone de los siguientes campos: «*Tipo de persona*», «*Tipo de Documento de Identificación*», «*Documento de Identificación*», «*Razón social*», «*Código de Directorios Unificado*», «*Nombre*», «*Primer apellido*» y «*Segundo apellido*».
Datos de contacto.	Tipo complejo (Datos Contacto).		Opcional.	Se compone de los siguientes campos: «*Dirección postal*», «*Dirección Electrónica Habilitada*», «*Correo electrónico*», «*Teléfono*» y «*Teléfono móvil*».
Receptor de notificaciones.	Booleano.		Opcional.	En escenarios con múltiples interesados y/o representantes, por medio de los valores booleanos «true» o «false», permite seleccionar expresamente cuál de los interesados o representantes será el que reciba las notificaciones. Tal y como el artículo 7 de la Ley 39/2015, por defecto, las notificaciones se remitirán al primer interesado que se consigne.
Canales de notificación y aviso.	Tipo complejo. (Canales Notificación).		Opcional.	De acuerdo con la Ley 39/2015, permite indicar preferencias en cuanto a los canales de recepción de notificaciones y avisos de notificaciones.
Tipo complejo: Datos Identificación.				
Tipo de persona.	Alfanumérico.	1	Obligatorio.	«1» = Persona física. «2» = Persona jurídica.

Segmento de Interesado				☑ Condicional ☑ Múltiple
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Tipo de Documento de Identificación.	Alfanumérico.	1	Obligatorio.	Identificación del interesado o representante: 'N' = NIF. 'C' = CIF. 'P' = Pasaporte. 'E' = Documento de identificación de extranjeros. 'X' = Otros de persona física. 'O' = Código de Origen.
Documento de Identificación.	Alfanumérico.	256	Obligatorio.	Alfanumérico con la sintaxis adecuada en función del campo «Tipo de Documento de Identidad».
Razón Social.	Alfanumérico.	80	Condicional.	Obligatorio si es persona jurídica.
Código de Directorios Unificados.	Alfanumérico.	21	Opcional.	Código del Interesado dentro de alguno de los Directorios Unificados contemplados en el Apartado VI.4 de esta norma. Dependiendo del directorio empleado, permitirá, entre otros, obtener información complementaria del interesado o identificar unidades dentro de la estructura jerárquica en la que se pueda descomponer el interesado.
Nombre.	Alfanumérico.	30	Condicional.	Obligatorio si es persona física.
Primer apellido.	Alfanumérico.	30	Condicional.	Obligatorio si es persona física.
Segundo apellido.	Alfanumérico.	30	Opcional.	
Tipo complejo: Datos Contacto.				
Dirección postal.	Tipo complejo. (Dirección Postal).		Condicional.	Se compone de los siguientes campos: «País», «Provincia», «Municipio», «Dirección» y «Código Postal». Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación.
Correo electrónico.	Alfanumérico.	160	Condicional.	Dirección de correo electrónico. Obligatorio cumplimentarlo si se solicita aviso de puesta a disposición de la notificación por correo electrónico.
Teléfono móvil.	Alfanumérico.	20	Condicional.	Obligatorio cumplimentarlo si se solicita aviso de puesta a disposición de la notificación por SMS.
Teléfono fijo.	Alfanumérico.	20	Opcional.	
Tipo complejo: Dirección Postal.				
País.	Alfanumérico.	4	Condicional.	Atributo según catálogo del INE. Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación.
Provincia.	Alfanumérico.	2	Condicional.	Atributo según catálogo del anexo de la OM del Padrón (11/7/1997). Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación y el país es España.
Municipio.	Alfanumérico.	5	Condicional.	Atributo según catálogo del anexo de la OM del Padrón (11/7/1997). Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación y el país es España.
Dirección.	Alfanumérico.	160	Condicional.	Dirección. Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación.
Código postal.	Alfanumérico.	5	Condicional.	Atributo según catálogo del anexo de la OM del Padrón (11/7/1997). Obligatorio cumplimentarlo si se establece el canal no telemático como canal preferente de notificación y el país es España.
Tipo complejo: Canales Notificación.				
Canal preferente de notificación.	Alfanumérico.	1	Opcional.	Permite indicar, en el caso de personas físicas, el canal preferente para la recepción de las notificaciones, de acuerdo con la Ley 39/2015: «1» = Notificación en papel. «2» = Notificación por medios electrónicos (siendo la administración quién, para cada trámite, decidirá si se efectúa por comparecencia en sede electrónica o en DEHú,o en ambas, pero debiendo ser en todo caso accesible desde el Punto de Acceso General).
Solicita aviso de notificación por SMS.	Booleano.		Opcional.	Permite al interesado indicar si desea recibir por este canal aviso de puesta a disposición de la notificación.
Solicita aviso de notificación por correo electrónico.	Booleano.		Opcional.	Permite al interesado indicar si desea recibir por este canal aviso de puesta a disposición de la notificación.

Tabla 3. Datos de Interesado

Los campos «Dirección postal», «Correo electrónico» o «Teléfono móvil» son condicionales de modo que, se pueden cumplimentar voluntariamente, en cualquier caso, pero deben cumplimentarse obligatoriamente si el canal de contacto en cuestión ha sido seleccionado expresamente en el campo «Canal preferente de notificaciones», en «Solicita aviso de puesta a disposición de la notificación por correo electrónico» o en «Solicita aviso de puesta a disposición de la notificación por SMS», respectivamente.

El campo «Canal preferente de notificaciones» no podrá tener el valor «1» para interesados obligados a relacionarse electrónicamente con las administraciones.

D) Segmento de Asiento.

Segmento de Asiento				☑ Obligatorio ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Modo de registro.	Alfanumérico.	2	Obligatorio.	"01" = Registro presencial en Oficina de Asistencia en Materia de Registro. "02" = Registro electrónico (desde sede electrónica, registros electrónicos generales o particulares u otros servicios electrónicos).

Segmento de Asiento				☑ Obligatorio ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Tipo del registro.	Alfanumérico.	1	Obligatorio.	"0" = Registro de entrada. "1" = Registro de salida.
Número de registro en la Entidad Registral de Origen o Inicio.	Alfanumérico.	20	Obligatorio.	Número de registro en la Entidad Registral de Origen o Inicio.
Fecha y hora de registro en Origen o Inicio.	Alfanumérico.	19	Obligatorio.	Formato AAAAMMDDHHMMSSZ.
Timestamp de registro en Origen o Inicio.	Alfanumérico.	Variable	Opcional.	Sello de tiempo del registro en Origen o Inicio.
Fecha y hora de presentación por el interesado.	Alfanumérico.	19	Obligatorio.	Formato AAAAMMDDHHMMSSZ. Coincidirá con la de registro si se registra en el mismo momento en el que se presenta por el interesado.
Timestamp de presentación por el interesado.	Alfanumérico.	Variable	Opcional.	Sello de tiempo de la presentación por el interesado.
«Abstract» o Resumen.	Alfanumérico.	240	Obligatorio.	
Código SIA.	Alfanumérico.		Opcional.	Código del procedimiento o servicio en el marco del cual se realiza la tramitación administrativa. Se obtendrá del Sistema de Información Administrativa.
Número de expediente.	Alfanumérico.		Opcional.	Número del expediente objeto de la tramitación administrativa. Deberá emplearse el formato normalizado de Identificador de expediente establecido en la NTI de Expediente Electrónico.
Código de asunto según destino.	Alfanumérico.	16	Opcional.	Codificación del asunto en destino, si la solicitud incluye ese dato. Se procurará definir solicitudes que incluyan el código para permitir el manejo automatizado del asiento en destino.
Referencia externa.	Alfanumérico.	16	Opcional.	Cualquier referencia que el destino precise conocer y sea conocida por el solicitante (matrícula de vehículo, número de recibo cuyo importe se reclama, etc.).
Otros metadatos generales.	Tipo complejo. (Metadatos).		Condicional.	Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del asiento que atiendan a necesidades generales.
Otros metadatos particulares.	Tipo complejo. (Metadatos).		Opcional.	Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del asiento que atiendan a necesidades particulares de la Unidad de Tramitación de Destino.
Tipo complejo: Metadatos.				
Campo.	Alfanumérico.	80	Opcional.	Nombre del metadato (general o particular) que se intercambia.
Valor.	Alfanumérico.	Variable	Opcional.	Valor del metadato (general o particular) indicado en el campo «Campo» anterior.

Tabla 4. Datos de Asunto

El formato de las fechas y horas de registro y presentación es yyyyMMddHHmmssZ, donde Z representa la variación en horas y minutos respecto a GMT (Ejemplo: 20200917124020+0200).

Los campos «Otros metadatos generales», «Otros metadatos particulares», «Campo» y «Valor» permiten intercambiar otros metadatos relativos al asiento adicionales a los ya transmitidos en campos nativos de la norma SICRES.

En el caso de «Otros metadatos generales», el listado de atributos a intercambiar (es decir, el listado de posibles contenidos del campo «Campo») será acordado y fijado por las Administraciones Públicas, con independencia de la aprobación de la NTI y pudiendo ser modificado a lo largo del tiempo. Los atributos de este listado podrán tener carácter opcional, condicional u obligatorio, por lo que deberán ser implementados por todas las Entidades Registrales.

En el caso de «Otros metadatos particulares», el listado de atributos a intercambiar (es decir, el listado de posibles contenidos del campo «Campo») será determinado por la Unidad de Tramitación de Destino que lo desee atendiendo a sus necesidades particulares, pudiendo establecerse un único listado a emplear por todos los orígenes, o listados particulares para determinados orígenes. Estos atributos serán siempre opcionales.

E) Segmento de Anexo.

Este segmento comprende datos e información relativa a los documentos electrónicos que son objeto de registro e intercambio. En el caso de justificantes de registro, su intercambio como documento anexo es opcional.

El segmento contiene la referencia única del documento electrónico a intercambiar. Esta referencia única consiste en un conjunto de campos con metadatos que permiten al destino la identificación unívoca del documento, la localización del repositorio en el que se encuentra almacenado y, en su caso, la acreditación de permisos para su acceso. Los campos y formatos de la referencia única del documento serán acordados y establecidos por las Administraciones Públicas al margen de esta NTI y pudiendo ser modificados a lo largo del tiempo. Esta información se recoge en la «Especificación del Sistema de referenciación de

documentos en las AAPP» del Foro por el Documento Electrónico – Documentación para la Tramitación Automatizada (https://administracionelectronica.gob.es/comunidades/verPestanaDocumentacion.htm?idComunidad=141).

Este segmento es opcional y puede declararse de forma múltiple.

Segmento de Anexo				**☑ Opcional ☑ Múltiple**
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Nombre del fichero anexado.	Alfanumérico.	80	Obligatorio.	Nombre del fichero original, incluyendo la extensión del fichero.
Identificador de fichero.	Alfanumérico.	50	Obligatorio.	Se compondrá siguiendo la normalización definida en el Anexo 1B.
Tipo de anexo.	Alfanumérico.	2	Obligatorio.	Indica el tipo de documento: – '01' = Justificante de registro. – '02' = Documento adjunto. – '03' = Otro.
Tipo MIME.	Alfanumérico.	80	Opcional.	Tipo del fichero Anexo.
Anexo.	Tipo complejo (Especificación del Sistema de referenciación de documentos en las AAPP).		Opcional.	Metadatos y referencia al documento electrónico registrado e intercambiado. Su estructura cumplirá la Especificación del Sistema de referenciación de documentos en las AAPP.
Resumen.	Alfanumérico.	160	Opcional.	Texto con descripción breve del contenido y naturaleza del anexo.
Código del formulario.	Alfanumérico.	80	Opcional.	Código del formulario o documento normalizado anexado.
Otros metadatos generales.	Tipo complejo. (Metadato).		Opcional.	Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del anexo que atiendan a necesidades generales.
Otros metadatos particulares.	Tipo complejo. (Metadato).		Condicional.	Secuencia de campos del tipo «Campo» y «Valor» empleados para transmitir atributos del anexo que atiendan a necesidades particulares de la Unidad de Tramitación de Destino.
Observaciones.	Alfanumérico.	160	Opcional.	Observaciones del fichero adjunto.
Tipo complejo: Metadato.				
Campo.	Alfanumérico.	80	Opcional.	Nombre del metadato (general o particular) que se intercambia.
Valor.	Alfanumérico.	Variable	Opcional.	Valor del metadato (general o particular) indicado en el campo «Campo» anterior.

Tabla 5. Datos de Anexo

F) Segmento de Internos y Control.

Segmento de Internos y Control				**☑ Obligatorio ☑ Único**
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Identificador de Intercambio.	Alfanumérico.	33	Obligatorio.	Identificador de Intercambio único de la operación. Se compondrá siguiendo la normalización definida en el Anexo 1 A.
Tipo de transporte de entrada.	Alfanumérico.	2	Opcional.	Formas de llegada al registro de entrada: – '01' = Servicio de Mensajeros. – '02' = Correo postal. – '03' = Correo postal certificado. – '04' = Burofax. – '05' = En mano. – '06' = Fax. – '07' = Otros. – '08' = Otros medios electrónicos.
Número de transporte de entrada.	Alfanumérico.	40	Opcional.	Referencia del transporte. Código. En el caso de certificados, número del mismo.
Nombre de usuario.	Alfanumérico.	80	Opcional.	Nombre del usuario de Origen.
Contacto de usuario.	Alfanumérico.	160	Opcional.	Contacto del usuario de Origen (teléfono o dirección de correo electrónico).
Aplicación y versión emisora.	Alfanumérico.	20	Opcional.	Identifica la aplicación y su versión.
Tipo de Anotación.	Alfanumérico.	2	Obligatorio.	Indica el motivo de la anotación (siguiendo la normalización definida en el apartadoV.2). Los únicos valores posibles para el mensaje de datos de intercambio son: – '01'= Pendiente (sin Identificador de Intercambio). – '02' = Envío. – '03' = Reenvío.
Descripción del Tipo de Anotación.	Alfanumérico.	160	Opcional.	
Documentación física y/o soportes.	Número.	1	Obligatorio.	Indica si el fichero va acompañado de documentación física. – '1' = Acompaña documentación física (u otros soportes) requerida. – '2' = Acompaña documentación física (u otros soportes) complementaria. – '3' = No acompaña documentación física ni otros soportes.
Observaciones del apunte.	Alfanumérico.	160	Opcional.	Observaciones del registro de datos de intercambio recogidos por el funcionario de registro.
Indicador de prueba.	Número.	1	Opcional.	Indica si el asiento registral es una prueba. – '0' = Normal. – '1' = Prueba.

Segmento de Internos y Control				☑ Obligatorio ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Identificador de intercambio previo.	Alfanumérico.	33	Opcional.	En caso de que el intercambio registral se trate de una rectificación de un intercambio previo, es decir, se trate de un envío como consecuencia de haber confirmado por error un registro recibido, este campo permitirá vincular este intercambio registral con el previo.
Código Entidad Registral de Inicio.	Alfanumérico.	21	Obligatorio.	Código único de la Entidad Registral de Inicio obtenido de Directorios Unificados indicados en el apartado VI.4.
Decodificación Entidad Registral de Inicio.	Alfanumérico.	120	Opcional.	Descripción de la Entidad Registral de Inicio.
Código de la Unidad de Tramitación de Inicio.	Alfanumérico.	21	Opcional.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4.
Decodificación de la Unidad de Tramitación de Inicio.	Alfanumérico.	120	Opcional.	Descripción de la Unidad de Tramitación Inicio.

Tabla 6. Datos de Internos y Control

Las consideraciones a tener en cuenta para asignar valor al campo ‘Documentación física y/o soportes’ son:

i. Acompaña documentación física (u otros soportes) requerida (‘1’). Indica que el mensaje de datos de intercambio debe ser tratado junto con documentación física (u otros soportes) necesaria para su trámite. Por tanto, no se puede aceptar y reenviar (si aplica) el fichero de intercambio hasta que toda la documentación física requerida haya sido recibida en la Entidad Registral de destino. Tampoco se puede dar número de registro oficial a la entrada, dándole temporalmente el tratamiento de ‘pre-asiento’, hasta disponer de la documentación física requerida.

Ejemplo de este caso, sería un intercambio en el que se realiza copia electrónica auténtica sólo de una parte de los documentos presentados, o cuando dichas copias no se pueden realizar (no se dispone de medios o el soporte no permite la digitalización correcta, como en el caso de sobres cerrados).

ii. Acompaña documentación física (u otros soportes) complementaria (‘2’). Indica que se envía documentación física (u otros soportes) que acompaña al mensaje de datos de intercambio, pero que ésta no es estrictamente necesaria para su trámite. Por tanto, se podría aceptar, pero no se podría reenviar (si aplica) el fichero de intercambio hasta que toda la documentación física haya sido recibida en la Entidad Registral de destino.

iii. No acompaña documentación física ni otros soportes (‘3’). Indica que el mensaje de datos de intercambio no se acompaña de ninguna documentación física ni otros soportes. Por tanto, se podría aceptar y reenviar (si aplica) el fichero de intercambio en cuanto llegue a la Entidad Registral de destino.

Además, este segmento incorpora la posibilidad de incluir información sobre la Entidad Registral de Inicio, cuya localización es necesaria para que un mensaje de datos de intercambio, que ha sido rechazado, pueda ser reenviado a la Entidad Registral que originó el proceso de intercambio, sin perder el rastro de la Entidad Registral que generó el reenvío. El modo en que el mensaje de datos de intercambio es reenviado a la Entidad Registral de Inicio se desarrolla en el apartado V de esta norma.

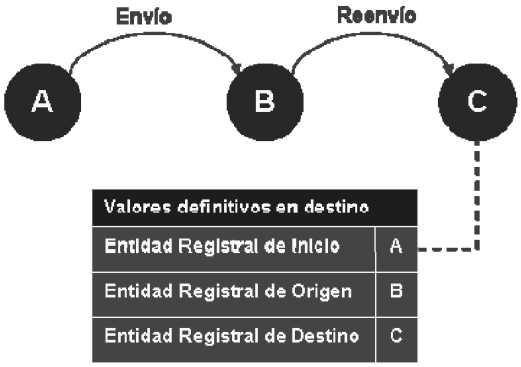


Figura 3. Diferenciación Entidad Registral de Inicio - Entidad Registral de Origen

Del mismo modo, el segmento incorpora también la posibilidad de incluir información sobre la Unidad de Tramitación de Inicio.

G) Segmento de Formulario Genérico.

Segmento de Formulario Genérico				☑ Opcional ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Expone.	Alfanumérico.	4000	Obligatorio.	Exposición de los hechos y antecedentes relacionados con la solicitud.
Solicita.	Alfanumérico.	4000	Obligatorio.	Descripción del objeto de la solicitud.

Tabla 7. Datos de Formulario Genérico

Este segmento opcional permite el intercambio del contenido de los formularios de propósito general que se implementan en los registros electrónicos.

Si se utiliza, además de incluir los datos específicos de este segmento, el formulario genérico se deberá incluir como documento anexo en el segmento de Anexo.

Esto permite que se puedan intercambiar formularios genéricos tanto con registros electrónicos con registros presenciales.

IV.3 Estructura y contenido del mensaje de control.

La entidad mensaje de control en SICRES 4.0 es un fichero que contiene la información de control y notificación acerca del estado de una operación de intercambio.

A continuación se definen los campos que componen un mensaje de control a utilizar, no así, el formato en que se implementen dentro del sistema de gestión de intercambio.

Segmento de Mensaje de Control				☑ Obligatorio ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Código Entidad Registral de Origen.	Alfanumérico.	21	Obligatorio.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4.
Código Entidad Registral de Destino.	Alfanumérico.	21	Obligatorio.	Código único obtenido de Directorios Unificados indicados en el apartado VI.4.
Identificador de Intercambio.	Alfanumérico.	33	Obligatorio.	Identificador de Intercambio único de la operación. Se compondrá siguiendo la normalización definida en el Anexo 1A.
Tipo de mensaje.	Alfanumérico.	2	Obligatorio.	Indica el tipo de mensaje (siguiendo la normalización definida en el apartado V.3). Los valores que el tipo de mensaje de control puede tomar son: – '01' = ACK (aceptación). – '02' = Error. – '03' = Confirmación. – '04' = ACK a Confirmación. – '05' = Rechazo. – '06' = ACK a Rechazo.
Descripción del mensaje.	Alfanumérico.	1024	Opcional.	Texto descriptivo del mensaje de control.
Número de registro de entrada en destino.	Alfanumérico.	20	Opcional.	Número de registro de entrada en la Entidad Registral destino. Utilizado para completar el ciclo de envío.
Fecha y hora de entrada en destino.	Alfanumérico.	19	Opcional.	Formato AAAAMMDDHHMMSSZ.

Segmento de Mensaje de Control				☑ Obligatorio ☑ Único
SICRES 4.0				
Descripción	**Tipo**	**Longitud**	**Obligación**	**Comentarios**
Indicador de prueba.	Número.	1	Obligatorio.	Indica si el mensaje es una prueba. – '0' =Normal. – '1' =Prueba.
Identificador de fichero.	Alfanumérico.	50	Opcional.	Identificador del mensaje de datos que se tiene que reenviar en caso de error. Se compondrá siguiendo la normalización definida en el Anexo 1 B, con tipo de fichero = '01' (anexo). Es opcional y múltiple, dado que el error puede producirse durante el envío de cualquiera de los ficheros: mensaje de datos de intercambio y Anexos (opcionales y múltiples).
Código de error.	Alfanumérico.	4	Opcional.	Identifica el tipo de error que se ha producido durante el envío del mensaje de datos de intercambio. Se compondrá siguiendo la normalización definida en el Anexo 1.D. Este valor sólo será aplicable en el caso de que el campo 'Tipo de Mensaje' tome el valor 'Error', codificado como '02'.

Tabla 8. Datos de Mensaje de control

V. Descripción y estados del intercambio

En este apartado se describen los posibles estados en los que se puede encontrar el apunte registral objeto del intercambio.

Tal y como se introdujo en el apartado IV.1, el proceso de intercambio inicia y finaliza en la Entidad Registral Origen, ya sea en el propio ciudadano o en la Unidad de Tramitación de Origen.

A lo largo de todo este proceso, Entidad Registral Origen y Destino se informan mutuamente sobre el estado del intercambio a través de sus respectivos campos:

i. Campo 'Tipo de anotación' del segmento de datos 'Internos y Control' del mensaje de datos de intercambio que emite la Entidad Registral Origen y destino.

ii. Campo 'Tipo de mensaje' de los mensajes de control que se envía.

De esta forma, el control sobre el estado del asiento registral a lo largo del proceso de intercambio se gestiona y controla de manera conjunta entre Origen y destino.

El inicio del intercambio viene marcado por la generación por parte de la Entidad Registral Origen del mensaje de datos de intercambio cuyo campo 'Tipo de anotación' tiene valor de *Pendiente.* El intercambio finaliza cuando, después de que la Entidad Registral de destino haya notificado a la Entidad Registral de Origen el asentimiento del intercambio enviándole un mensaje de control de tipo *confirmación,* esta Entidad Registral de Origen acepta el mensaje devolviéndole a la Entidad Registral de Destino un mensaje de control de tipo *ack.*

Las Entidades Registrales deben implementar mecanismos y procedimientos que eviten la duplicación de asientos en caso de recepciones múltiples. Las herramientas para esta implementación son los datos 'Identificador de Intercambio', 'Identificador de Fichero' y 'Número de Secuencia'.

V.1 Generación del Identificador de Intercambio.

La aplicación de registro de la Entidad Registral Origen que interviene en el proceso de intercambio, es responsable de la generación de un identificador de intercambio único para cada operación en el espacio de intercambio del tipo:

<Código Entidad Registral Origen>_<AA>_<Número Secuencial>

Este identificador se mantiene durante todo el proceso de intercambio tanto en el sistema de gestión de intercambio como en la aplicación de registro de la Entidad Registral destino. En el apartado Anexo 1A se describen las reglas para la generación de este identificador.

V.2 Estados en el mensaje de datos de intercambio.

Los estados que registra el mensaje de datos de intercambio en el campo de 'Tipo de anotación' son:

i. Pendiente ('01'): Indica que el mensaje de datos de intercambio está pendiente de envío al sistema de intercambio y que está pendiente de la asignación de un identificador del intercambio para iniciar el proceso.

ii. Envío ('02'): Indica que el mensaje de datos de intercambio está en pleno proceso de intercambio, y por tanto, ha partido desde la Entidad Registral de Origen pero está pendiente aún de convertirse en registro en firme por la Entidad Registral de destino.

iii. Reenvío ('03'): Indica que el mensaje de datos de intercambio es enviado de nuevo desde la Entidad Registral de destino.

La razón para el reenvío es, generalmente, que el destino indicado en el primer envío no corresponde. Cuando se da esta situación, la Entidad Registral de destino puede identificar la Entidad Registral de destino correcta y reenviarlo a ésta en lugar de rechazar el envío que realizó la Entidad Registral Origen.

Esta secuencia de envíos y los valores que toma el campo 'Tipo de anotación' aparecen en la siguiente figura.

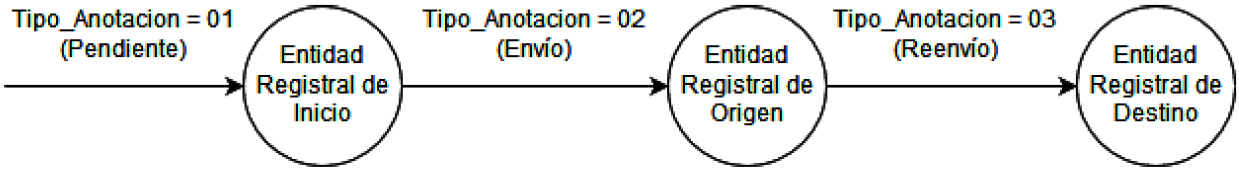


Figura 4. Tipo de anotación en mensaje de datos de intercambio en caso de reenvío

V.3 Estados en los mensajes de control.

La información de estado del intercambio que se refleja en los mensajes de control a través de los siguientes valores de 'Tipo de mensaje':

i. ACK-aceptación ('01'): Notifica la recepción correcta del mensaje de datos de intercambio desde un punto de vista exclusivamente técnico, por lo que no constituye la confirmación de finalización correcta de todo el proceso de intercambio.

A continuación, se muestra una figura explicativa de la emisión de un mensaje de control tipo aceptación:

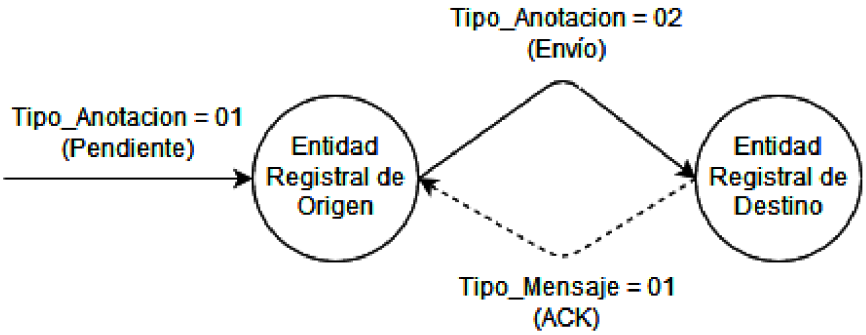


Figura 5. Emisión de mensaje de control ACK tras la recepción correcta del mensaje de datos de intercambio

Los mensajes de control de aceptación deberán emitirse también para notificar la recepción correcta desde el punto de vista técnico de los mensajes de control de tipo confirmación. En la figura 10 se muestra la emisión de este mensaje en tal escenario.

ii. Error ('02'): Notifica la recepción errónea o incompleta del mensaje de datos de intercambio desde un punto de vista técnico. Los posibles tipos de errores que se pueden dar se identifican mediante un rango de error y el propio código de error. Este mensaje de control refleja el tipo de error a través de la codificación de errores que se detalla en el Anexo 1.D.

La siguiente figura refleja la emisión de un mensaje de control tipo Error:

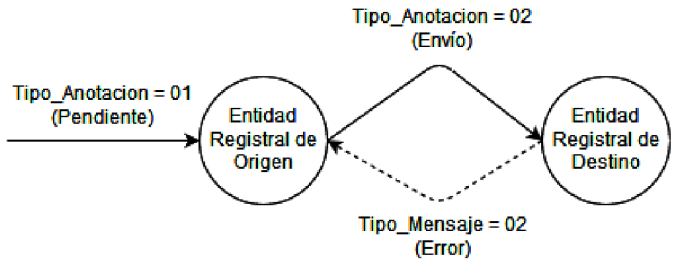


Figura 6. Emisión de mensaje de control tipo Error tras la recepción errónea del mensaje de datos de intercambio

Ante esta situación, la Entidad Registral de Origen ('A') puede enviar el mensaje de datos de intercambio a la Entidad Registral de destino ('B'), reenviarlo o rechazarlo.

iii. Confirmación ('03') y ACK Confirmación ('04'): Una vez recibido el mensaje de datos de intercambio y todos sus documentos anexos, se acepta que el proceso de intercambio se ha realizado con éxito y, por tanto, se notifica a la Entidad Registral de Origen o Inicio que la recepción ha sido correcta confirmando por tanto el asentimiento del intercambio completado.

La figura que sigue, muestra la secuencia que provoca la emisión de un mensaje de control tipo confirmación y la correspondiente aceptación de la confirmación:

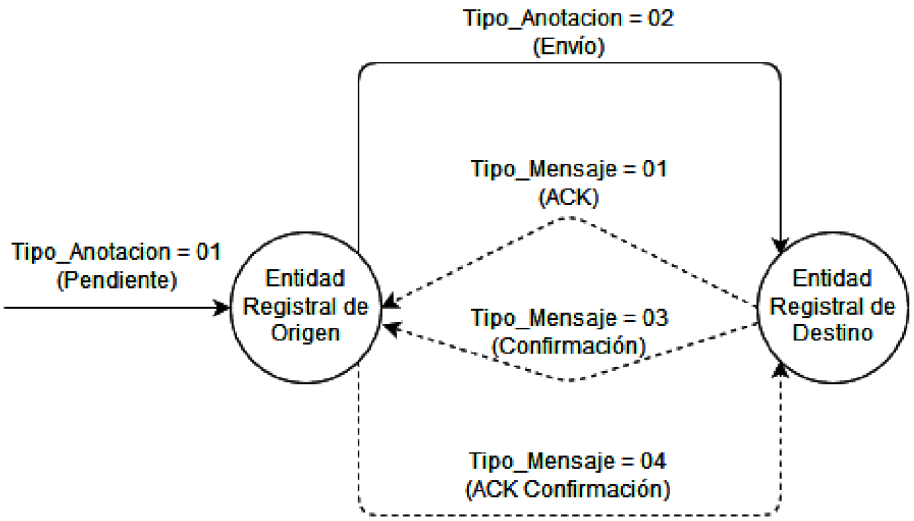


Figura 7. Envío de mensaje de control tipo Confirmación tras la recepción correcta del mensaje de datos de intercambio y sus anexos

El asentimiento es necesario para el correcto funcionamiento de los flujos de intercambio definidos, por lo que debe ser implementado por todas las Entidades Registrales para el intercambio de los asientos. El asentimiento permite confirmar que el asiento registral es correcto y corresponde a la Entidad Registral de destino por lo que debe emitirse tanto tras la recepción de un mensaje de datos de intercambio con 'Tipo de anotación' envío como si se trata de un *reenvío*.

La Entidad Registral de Destino deberá reenviar el Mensaje de Control de confirmación si pasado un periodo de tiempo (predefinido en cada sistema de intercambio) no recibe de la Entidad Registral de Origen o Inicio el Mensaje de Control de *ACK Confirmación.*

iv. Rechazo ('05') y ACK Rechazo ('06'): Indica que el mensaje de datos de intercambio no ha sido aceptado por la Entidad Registral de destino.

En caso de rechazo, el mensaje de datos de intercambio será enviado siempre a la Entidad Registral de Inicio.

La Entidad Registral de Destino deberá reenviar el Mensaje de Control de rechazo si pasado un periodo de tiempo (predefinido en cada sistema de intercambio) no recibe de la Entidad Registral de Inicio el Mensaje de Control de ACK Rechazo.

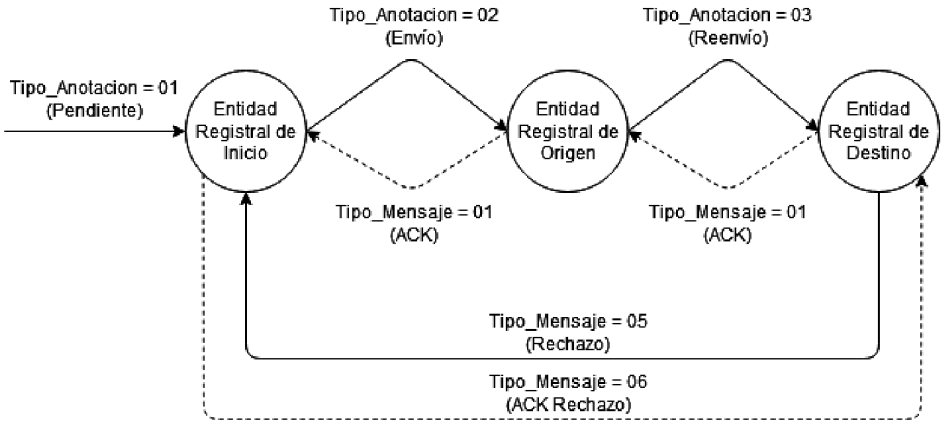


Figura 8. Tipo de anotación en mensaje de datos de intercambio en caso de rechazo

VI. Funciones y requisitos del sistema de intercambio.

El sistema de intercambio utilizado para emisión y recepción de los mensajes definidos en los apartados anteriores funciona, en el espacio de intercambio SICRES, como elemento responsable de:

i. Centralizar el registro de operaciones de intercambio y garantizar la trazabilidad de las mismas.
ii. Gestionar la situación temporal de los 'pre-asientos registrales'.
iii. Proporcionar la seguridad en el transporte de la información a través de mecanismos de encriptación en el mensaje de datos de intercambio.
iv. Firma electrónica del mensaje de datos de intercambio.

Como ya se ha indicado, esta norma no establece los requisitos tecnológicos concretos que deben proporcionar el sistema que da soporte a un intercambio de asientos registrales, ya que SICRES4.0 es independiente de la tecnología o plataforma sobre la que se realice la transmisión de los elementos que forman el intercambio propiamente dicho.
No obstante, sí se establecen unos principios básicos que deben ser cubiertos por el sistema de intercambio que se utilice, como son:

i. Integridad: Garantía de que la información no es modificada en los procesos de intercambio.
ii. Confidencialidad: Disponibilidad de la información solamente para usuarios autorizados.
iii. Autenticidad: Legitimidad del origen de la información.
iv. No repudio: Imposibilidad de negación ante terceros del envío y/o recepción por parte del emisor y/o receptor de la información.
v. Accesibilidad: Posibilidad de acceso eficiente sólo para entidades autorizadas.

A continuación se desarrollan estos requisitos de seguridad y, posteriormente, las funciones que debe proporcionar el sistema de intercambio.

VI.1 Requisitos de seguridad.

a) Autenticación de los sistemas implicados.

Además de la implementación de las políticas de seguridad para los usuarios de la plataforma de intercambio, se asegura la identidad de cada uno de los sistemas intervinientes en el espacio de intercambio.
Así, todos los sistemas que participen en el proceso de intercambio, incluidos los sistemas de las Entidades Registrales de Origen y Destino, están correctamente identificados y validados en el espacio de intercambio.

b) Integridad.

La plataforma de intercambio proporciona los mecanismos necesarios, a fin de garantizar que el contenido completo de los mensajes de datos intercambiados permanezca inalterado durante el proceso de intercambio.

Este punto se asegura a través del protocolo de transporte de mensajes entre las Entidades Registrales de Origen y Destino que utilice el sistema de intercambio, y la tecnología de transmisión de datos.

c) Garantía de no repudio.

La plataforma de intercambio provee de los mecanismos necesarios para garantizar el no repudio del mensaje de datos de intercambio.

VI.2 Gestión del proceso de intercambio.

Como ya se ha mencionado, para iniciar el intercambio, la aplicación de registro de la Entidad Registral Origen genera el mensaje de datos de intercambio de forma completa y lo envía al sistema de gestión de intercambio.

La plataforma de intercambio es responsable de verificar la validez del mensaje de datos de intercambio según el formato establecido en esta norma.

Además, el sistema de gestión de intercambio es el encargado de garantizar la transmisión entre los sistemas de la Entidad Registral Origen y destino.

Posteriormente, la aplicación de registro de la Entidad Registral destino es la responsable de interpretar de forma correcta el fichero intercambiado.

Hasta que el intercambio concluye, la plataforma de intercambio tiene la misión de resolver de forma correcta la situación temporal del 'pre-asiento registral' que desaparece cuando se produce la recepción completa de todos los ficheros que pudieran constituir un envío.

Dentro de cada espacio de intercambio debe definirse un conjunto de reglas que permitan la gestión del intercambio entre Entidades Registrales a través de un sistema de intercambio. Estas reglas permiten definir los mecanismos y herramientas para realizar el intercambio en condiciones adecuadas incluyendo:

i. La tecnología de comunicación entre los distintos agentes del intercambio.

ii. Los mecanismos y procedimientos específicos para el envío y recepción de ficheros, y para garantizar la integridad y seguridad de los envíos.

iii. Las políticas específicas de protección de datos que deben ser de aplicación.

iv. Los mecanismos de trazabilidad de los intercambios y la información que se registre sobre los mismos.

v. Procedimientos detallados de gestión de errores y excepciones.

a) Gestión de envíos de mensajes y anexos.

La plataforma de intercambio debe realizar una gestión adecuada del envío de mensajes y los posibles documentos anexos asociados, que garantice la correcta identificación del registro completo en la Entidad Registral de destino y su posterior almacenamiento.

b) Gestión del flujo.

Las operaciones de intercambio tienen definido un estado (definidos en el apartado V de la presente norma) en el que se indica la fase lógica dentro del proceso de intercambio en la que se encuentra el fichero, y los posibles eventos que pueden ocurrir.

c) Evitar duplicados.

El sistema de gestión de intercambio contiene los mecanismos necesarios para garantizar que los asientos que se envíen o reciban por duplicado de manera errónea, sean identificados como tales.

Las Entidades Registrales deben implementar mecanismos y procedimientos que eviten la duplicación de asientos en caso de que se reciban varias veces, utilizando los datos 'Identificador de Intercambio', 'Identificador de Fichero' y 'Número de Secuencia'.

d) Gestión de mensajes.

El sistema de intercambio dispone de funcionalidades de gestión de mensajes de actividad, a fin de proporcionar información de seguimiento a la Entidad Registral de Origen, una vez realizado el intercambio, tal y como se describe en el apartado V.

La gestión y conservación de los anexos, entendidos éstos como documentos electrónicos, se definen y normalizan en la *NTI de Política de gestión de documentos electrónicos.*

e) Conservación de la información del asiento registral.

Cuando los pre-asientos registrales intercambiados no se convierten en asientos firmes en la Entidad Registral de destino, ésta no debe conservar el mensaje de datos de intercambio ni sus documentos adjuntos. Únicamente debe conservar traza de la transacción de intercambio realizada.

VI.3 Soporte del modo de prueba.

El sistema de gestión de intercambio debe disponer de la capacidad de soportar el modo de prueba en el proceso de intercambio, de tal forma que permita realizar pruebas de intercambio.

El modelo de datos incluye un identificador para mensajes de datos de intercambio que indica que son una prueba que aparece detallado en los apartados IV.2 y IV.3.

VI.4 Directorios unificados de organismos, entidades y unidades.

En el sistema de intercambio se deberán emplear códigos de identificación unívoca de las Entidades Registrales y Unidades de Tramitación que actúan como emisoras o receptoras de asientos registrales (campos de Entidades Registrales y Unidades de Tramitación de los segmentos «De Origen», «De Destino» y «De internos y control»). Para ello, podrán emplearse los siguientes directorios unificados:

i. Directorio Común de Unidades Orgánicas y Oficinas (DIR3): directorio que, cumpliendo con el artículo 9 del Real Decreto 4/2010, codifica de forma unívoca, tanto los organismos, órganos y unidades de tramitación de las administraciones públicas, como las Oficinas de Registro y atención al ciudadano, y mantiene información sobre ellos y las relaciones entre ellos.

ii. Directorio de Entidades (DIRe): directorio que mantiene información sobre personas jurídicas del ámbito privado y su estructura organizativa, asignando códigos de identificación unívoca a las posibles unidades de tal estructura.

iii. Otros directorios unificados que puedan crear y acordar las administraciones públicas.

Los códigos de estos directorios podrán también ser empleados para identificar y facilitar la obtención de información complementaria o adicional sobre los interesados (campo «Código de Directorios unificados» del «Segmento de Interesado»).

VI.5 Control y gestión de errores.

La plataforma de intercambio es responsable de realizar una gestión adecuada de los errores y excepciones que puedan ocurrir durante el proceso de intercambio, que facilite la restauración de información en la medida de lo posible.

a) Tipología de errores de intercambio.

Los principales errores que pueden ocurrir durante el intercambio registral pueden clasificarse, en base a la naturaleza del error, como:

i. Errores lógicos: relativos a errores en las validaciones en estructura y/o en contenido de los ficheros de intercambio y/o en direcciones de origen o destino. En definitiva, cualquier error no achacable a un problema tecnológico, pero que provoca que el resultado del intercambio no sea exitoso.

ii. Errores físicos: relativos a errores que se pueden asociar con la tecnología que interviene en el proceso de intercambio, como la no disponibilidad de máquinas, de elementos de la infraestructura de software, excepciones de código no controladas y otros.

iii. Errores de transmisión de datos: relativos a errores que pueden ocurrir durante la transmisión de datos debido a problemas en las comunicaciones.

La codificación de los errores aparece en el Anexo 1.D.

Tipo de error		Definición
Errores lógicos.	Errores de validación de los datos de intercambio.	Ocurren al resultar erróneas las validaciones lógicas de los datos del intercambio en formatos, datos requeridos y correspondencia entre descripciones de contenido y el contenido de los datos de intercambio.
	Errores de direccionamiento.	Ocurren cuando la identidad del remitente o destinatario reflejada en el mensaje de datos de intercambio no se corresponde con el que debería enviar o recibir la información.
	Errores en las reglas de intercambio.	Aparece un evento no esperado durante el intercambio registral.
	Errores de ciclo de envío no completado.	No se puede completar el ciclo de envío completamente.
Errores físicos.		Se producen cuando ocurren errores, hardware o software, en alguno de los sistemas intervinientes.
Errores de transmisión de datos.		No se puede producir el intercambio, debido a que el sistema de destino o el de Origen no están disponibles.

Tabla 9. Descripción de errores de intercambio

b) Errores lógicos.

Descripción de los errores lógicos:

i. Errores de validación de los datos de intercambio. Ocurren al resultar erróneas las validaciones lógicas de los datos del intercambio en formatos, datos requeridos y correspondencia entre descripciones de contenido y el contenido de los datos de intercambio.

ii. Errores de direccionamiento. Ocurren cuando la identidad del remitente o destinatario reflejada en el mensaje de datos de intercambio no se corresponde con el que debería enviar o recibir la información.

iii. Errores en las reglas de intercambio. Aparece un evento no esperado durante el intercambio registral.

iv. Errores de ciclo de envío no completado. No se puede completar el ciclo de envío completamente.

Tratamiento de los errores lógicos:

i. Errores de validación de los datos de intercambio. En el momento que se detecte esta falta de integridad en los datos de intercambio, se deberá interrumpir el proceso marcando como erróneo el mensaje de datos de intercambio. A continuación se deberá notificar al Origen de que no se ha podido interpretar correctamente los datos, informándole del código de error lógico ocurrido.

Una vez notificado, la Entidad Registral de Origen se dispondrá a analizar la naturaleza del error para realizar acciones de subsanación:

1. Si es relativo a una composición errónea del mensaje de datos de intercambio y anexos asociados, deberá recomponerlos y retransmitirlos.

2. Si el error es debido a una corrupción de datos durante la transmisión deberá simplemente retransmitirlos.

La operación deberá ser registrada como errónea en el log de operaciones del sistema de gestión del intercambio.

ii. Errores de direccionamiento. Se pueden producir por errores en la dirección del remitente o en el destinatario.

Si se produce un error en los datos del destinatario, es posible que sucedan dos escenarios:

1. Los datos llegan a una Entidad Registral de destino no esperada. En este caso, la Entidad destino deberá rechazar el registro recibido y notificar a la Entidad Origen de la ocurrencia de este suceso a través del sistema de gestión de intercambio.

2. Los datos llegan a un destino no esperado fuera del espacio de intercambio registral, es decir, no es enviado a una Entidad Registral. El error se podrá identificar por un aviso de error de direccionamiento proporcionado por el sistema de gestión de intercambio (por ejemplo ‘destino inalcanzable’), o al no recibirse la confirmación de la entrega pasado un tiempo preestablecido por parte de la Entidad Registral de Origen.

El tratamiento de estos errores se llevaría a cabo a través de la realización retransmisiones desde el sistema de intercambio o desde la Entidad Registral Origen, una vez solucionado el error de direcciones.

Si se produce un error en los datos del remitente, es posible que sucedan dos escenarios:

1. Se recibe una confirmación de entrega en una Entidad Registral de Origen no esperada. En este caso, la Entidad Origen deberá rechazar la confirmación.

2. La confirmación de entrega es enviada a una dirección fuera del espacio de nombres del intercambio registral. En este caso el error se detectará si la entidad Origen no recibe la confirmación de la entrega en un tiempo preestablecido o si al enviar la confirmación se produce un aviso de error de direccionamiento, por ejemplo 'destino inalcanzable'.

Para tratar los errores de destinatario se intentarán retransmisiones desde el sistema de intercambio o desde la Entidad Registral destino, una vez solucionado el error de direcciones.

Los errores de direcciones pueden estar motivados por entradas erróneas en el Directorio Común. En estos casos, se debe detectar (normalmente al aparecer errores de direccionamiento) y realizar la corrección de la entrada incorrecta.

Las operaciones anteriormente indicadas deberán ser registradas como erróneas en el log de operaciones del sistema de gestión de intercambio.

iii. Errores en las reglas de intercambio. Este error ocurrirá si aparece un evento no esperado durante el intercambio registral (por ejemplo, se recibe un segundo mensaje de control de confirmación de entrega correcta para un mismo Identificador de Intercambio).

En este caso, el sistema de gestión de intercambio se vuelve inconsistente, por lo que se deberá registrar el elemento que ha producido el evento, y realizar una notificación para solucionar el problema.

iv. Errores de ciclo de envío no completado. Este error ocurrirá si no se hubiera podido cerrar el ciclo de envío completo, al interrumpirse en alguno de sus pasos. Se detecta al sobre pasarse los límites de tiempo esperados para que un paso del ciclo se realice.

El Origen de este error puede ser variado, debido tanto a problemas lógicos como físicos. El tratamiento normal para estos casos es la retransmisión de los datos.

La operación errónea deberá ser registrada en el log del sistema de gestión de intercambio, indicando los reintentos efectuados y si fueron exitosos o no. Si al efectuar el número de reintentos determinado no se consiguiera cerrar el ciclo, el conjunto de datos objeto del error deberá ser marcado como erróneo notificando a el sistema de intercambio, la necesidad de un tratamiento para su subsanación.

c) Errores físicos.

Descripción de los errores físicos:

Se producen cuando ocurren errores, hardware o software, en alguno de los sistemas intervinientes.

Tratamiento de los errores físicos:

Los errores en el sistema de intercambio deben ser tratados según los procedimientos de operación que apliquen en cada caso.

Las operaciones de intercambio que se viesen afectadas por el error ocurrido se identificarán y restaurarán en la medida de lo posible.

d) Errores de transmisión.

Descripción de los errores de transmisión:

No se puede producir el intercambio, debido a que el sistema de destino o el de Origen no están disponibles.

Tratamiento de los errores de transmisión:

Si alguno de los sistemas no está disponible el tratamiento normal será la realización de reintentos de envío.

La operación errónea deberá ser registrada en el log del sistema de gestión de intercambio, indicando los reintentos efectuados y si fueron exitosos o no. Si al efectuar el número de reintentos establecidos no se consiguiera cerrar el ciclo, el conjunto de datos objeto del error deberá ser marcado como erróneo notificando al sistema de gestión de intercambio de la necesidad de un tratamiento para su subsanación.

VII. Otras recomendaciones

Existen otros requerimientos de tecnología que pueden ser considerados como recomendaciones.

a) Registro de la actividad de intercambio.

Se recomienda, que el estado y la secuencia de las operaciones de intercambio se registren en un sistema centralizado del sistema de intercambio, que permita realizar la trazabilidad de las operaciones efectuadas.

Las aplicaciones de registro de las Entidades Registrales implicadas en un proceso de intercambio, podrán hacer uso de los datos de trazabilidad para proporcionar un servicio de seguimiento a los ciudadanos e instituciones que lo soliciten.

b) Persistencia en errores y excepciones.

Los datos del mensaje de datos de intercambio y el estado de sus operaciones a través del sistema de gestión de intercambio, deberían permanecer en un medio persistente cuando se produzcan errores o excepciones que impidan su envío/recepción. Se garantizará la perdurabilidad de registro y su estado, si ocurrieran errores en el proceso de intercambio.

ANEXO 1

Codificación

ANEXO 1A

Identificador del intercambio

A cada operación de intercambio se le asocia un identificador que permite designar la operación de forma única.

<Código Entidad Registral Origen>_<AA>_<Número Secuencial>

La codificación de este identificador se compone según el siguiente criterio:

Campo	Definición / Valor
<Código Entidad Registral Origen>.	Código que figura para la Entidad Origen en Directorios Unificados indicados en el apartado IV.4, codificado en base a 21 caracteres.
<AA>.	Año en curso en dos dígitos.
<Número Secuencial>.	Con una longitud de 8 dígitos, suficiente para evitar que puedan repetirse dos Identificadores en la misma Entidad Registral.

Tabla 10. Formato del identificador del intercambio

La generación de este código se realiza antes de enviar el Mensaje de datos de intercambio, al sistema de gestión de intercambio.

ANEXO 1B

Identificadores de ficheros de mensajes de datos de intercambio y anexos

En el proceso de intercambio se transmiten diferentes ficheros entre Origen y Destino. Por un lado, a través de la Plataforma de Intercambio, se transmiten ficheros con Mensajes de Datos de Intercambio y Mensajes de Control. Además, haciendo uso de las interfaces y

canales habilitadas por los repositorios del sistema de referencias únicas, se transmiten ficheros con documentos electrónicos en formato ENI que contiene los documentos anexos.

Todos estos ficheros deben ser intercambiados con nombres de acuerdo con un formato normalizado. El uso de esta notación permite identificar de forma única a los ficheros dentro del espacio de intercambio registral.

A continuación se muestra el formato del nombre que deben tener los ficheros de Mensajes de Datos de Intercambio y de fichero de Anexos:

<Identificador del Intercambio>_<Código de tipo de archivo>_<Número Secuencial>.<Extensión del fichero>

Campo	Definición / Valor
<Identificador del Intercambio>.	Se genera tal y como se indica en el apartado anterior (Anexo 1 A). Por tanto, este campo, a su vez, tendrá el formato: <Código Entidad Registral Origen>_<AA>_<Número Secuencial>
<Código de tipo de archivo>.	00 = Mensaje SICRES: indica que el fichero es un mensaje de datos de intercambio. 01 = Anexo: indica que el fichero es un anexo.
<Número secuencial>.	Hasta cuatro dígitos y la secuencia puede reiniciarse con cada proceso de intercambio que tenga un identificador de intercambio diferente.
<Extensión del fichero>.	Formato que se determine para el intercambio.

Tabla 11. Formato del identificador de los ficheros de Mensajes de Datos de Intercambio y de Anexos

ANEXO 1C

Identificador de ficheros de mensajes de control y notificación

Los ficheros de los Mensajes de Control se nombrarán de acuerdo con la siguiente estructura:

<Código de la Entidad Registral Emisora>_<AA>_<Número Secuencial>.>.<Extensión del fichero>

Campo	Definición / Valor
<Código de la Entidad Registral Emisora>.	Código obtenido de Directorios Unificados indicados en el apartado IV.4 de la Entidad Registral que crea el mensaje, codificado en base a 21 caracteres.
<AA>.	Indica el año en curso, con una longitud de 2 dígitos.
<Número Secuencial>.	Con una longitud de 8 dígitos, suficiente para evitar que puedan repetirse dos identificadores en la misma Entidad Registral.
<Extensión del fichero>.	Formato que se determine para el intercambio.

Tabla 12. Formato del Identificador de fichero del Mensaje de control y notificación

ANEXO 1D

Errores

Para realizar la codificación de los errores del sistema de intercambio, se utiliza un código de cuatro dígitos, estructurado en dos niveles:

i. Rango de error, que agrupa la definición de un tipo general de error. Se codifica con los dos primeros dígitos y establecen una secuencia:

0000
0100
0200
…
9900

ii. Código de error, pertenecientes a un rango. Utilizando los dos últimos dígitos, de la siguiente forma:

0000
0001
0002
…
0099

Por ejemplo, se puede definir un rango de error del tipo:

‘0000’ Errores en la validación del mensaje de datos de intercambio.

Y definir un error concreto como:

‘0001’ No se incorporan los anexos definidos en el mensaje de datos de intercambio.

ANEXO 2

Ejemplo esquema XML del modelo de datos SICRES 4.0

El objetivo de este anexo es mostrar el modelo de datos SICRES 4.0 en formato de esquema XML. Se adjuntarán ficheros XML de ejemplo.

Representación gráfica del esquema del mensaje de datos de intercambio

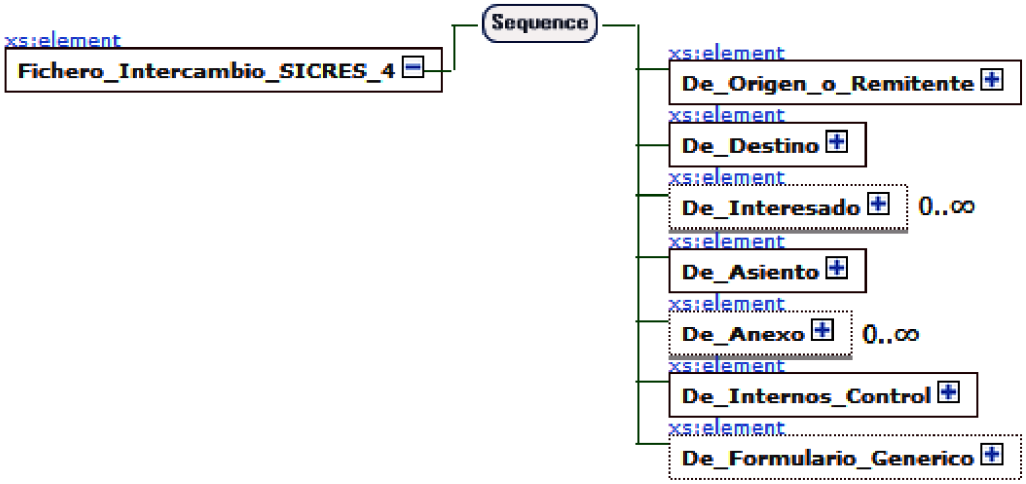


Figura 9. Esquema XML: Mensaje de datos de intercambio - Visión general

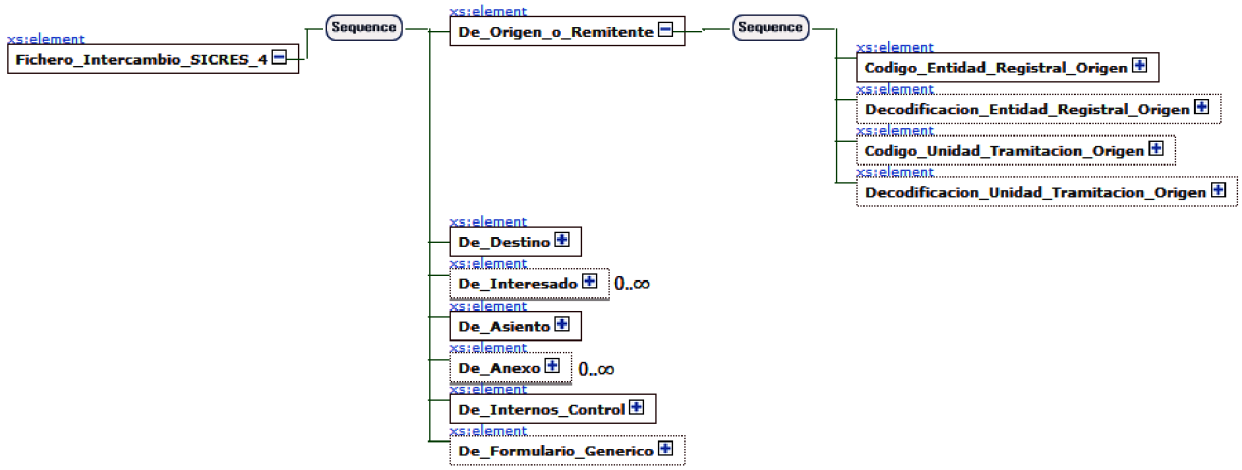


Figura 10. Esquema XML: Mensaje de datos de intercambio - Detalle de Origen o Remitente

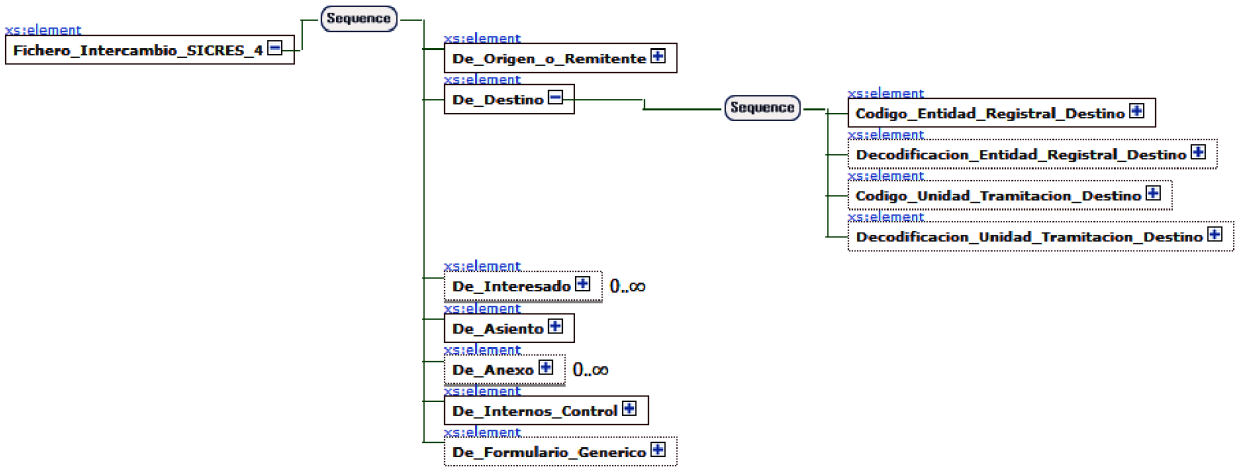


Figura 11. Esquema XML: Mensaje de datos de intercambio - Detalle de destino

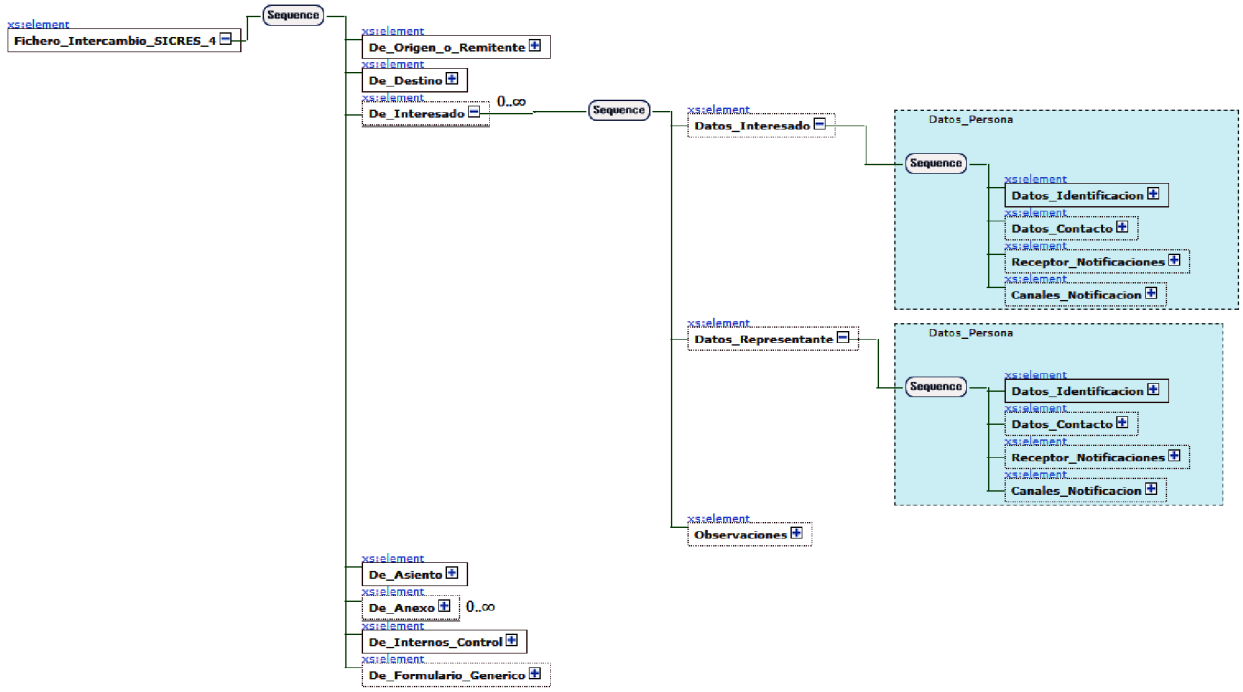


Figura 12. Esquema XML: Mensaje de datos de intercambio - Detalle de Interesado

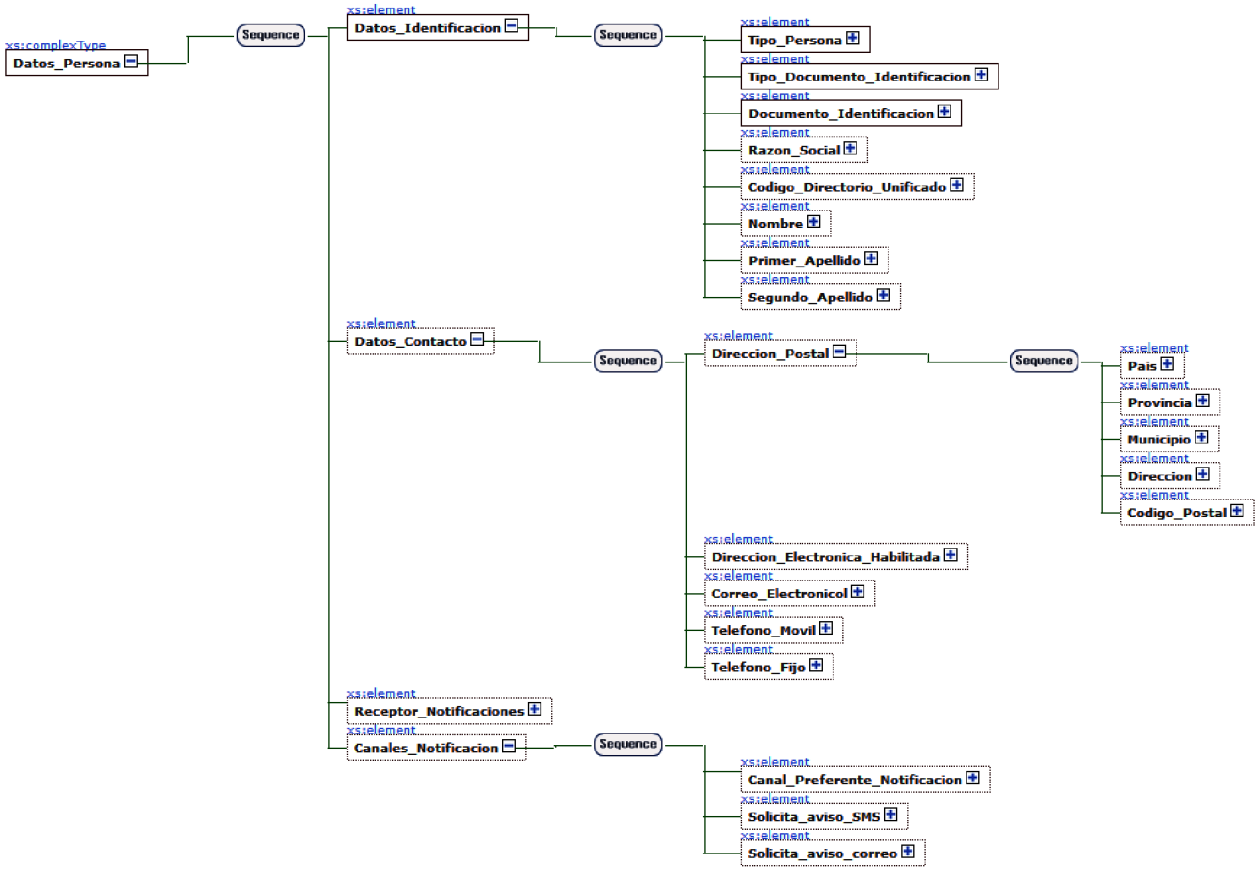


Figura 13. Esquema XML: Mensaje de datos de intercambio - Detalle de Datos de Persona

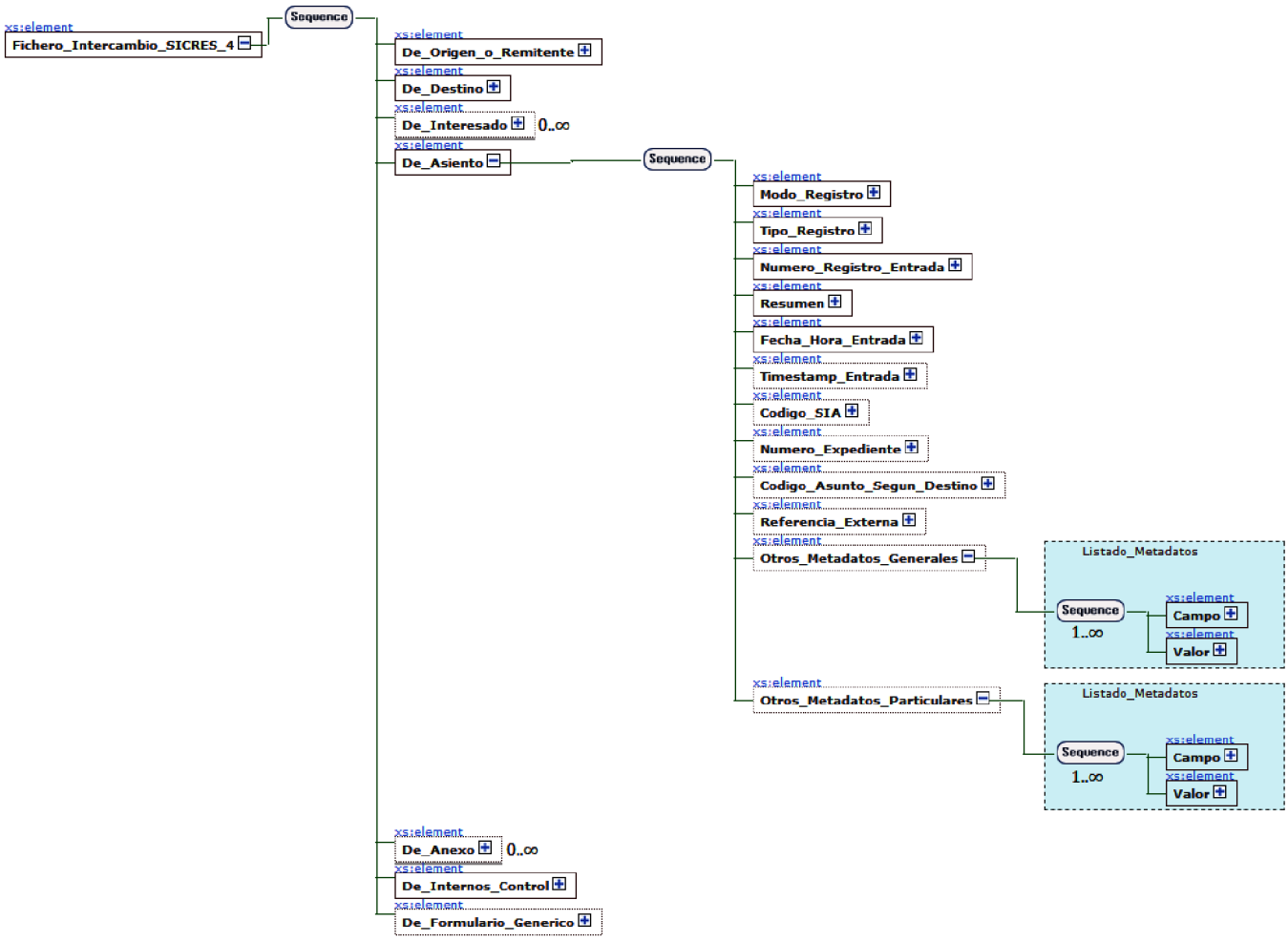


Figura 14. Esquema XML: Mensaje de datos de intercambio - Detalle de Asiento

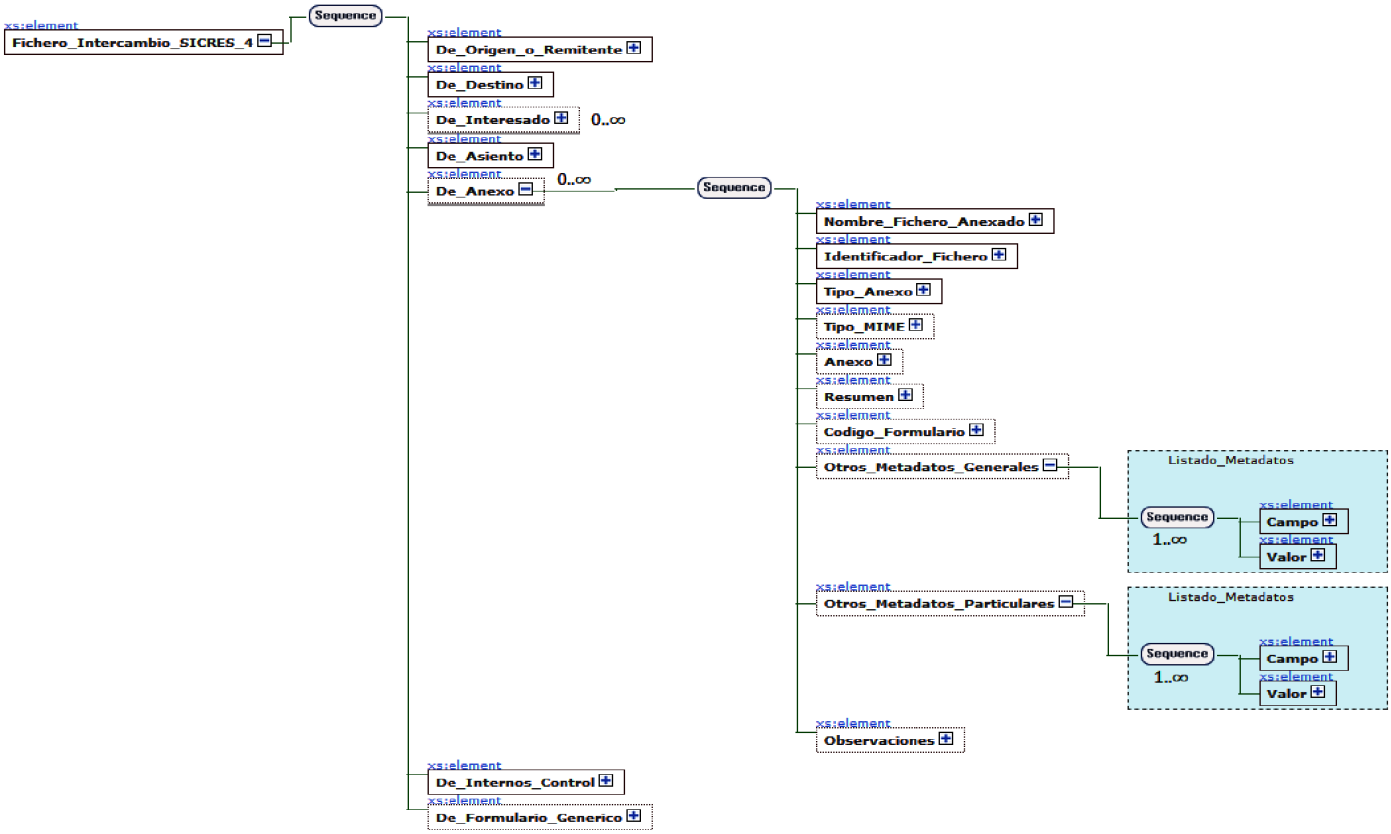


Figura 15. Esquema XML: Mensaje de datos de intercambio - Detalle de Anexo

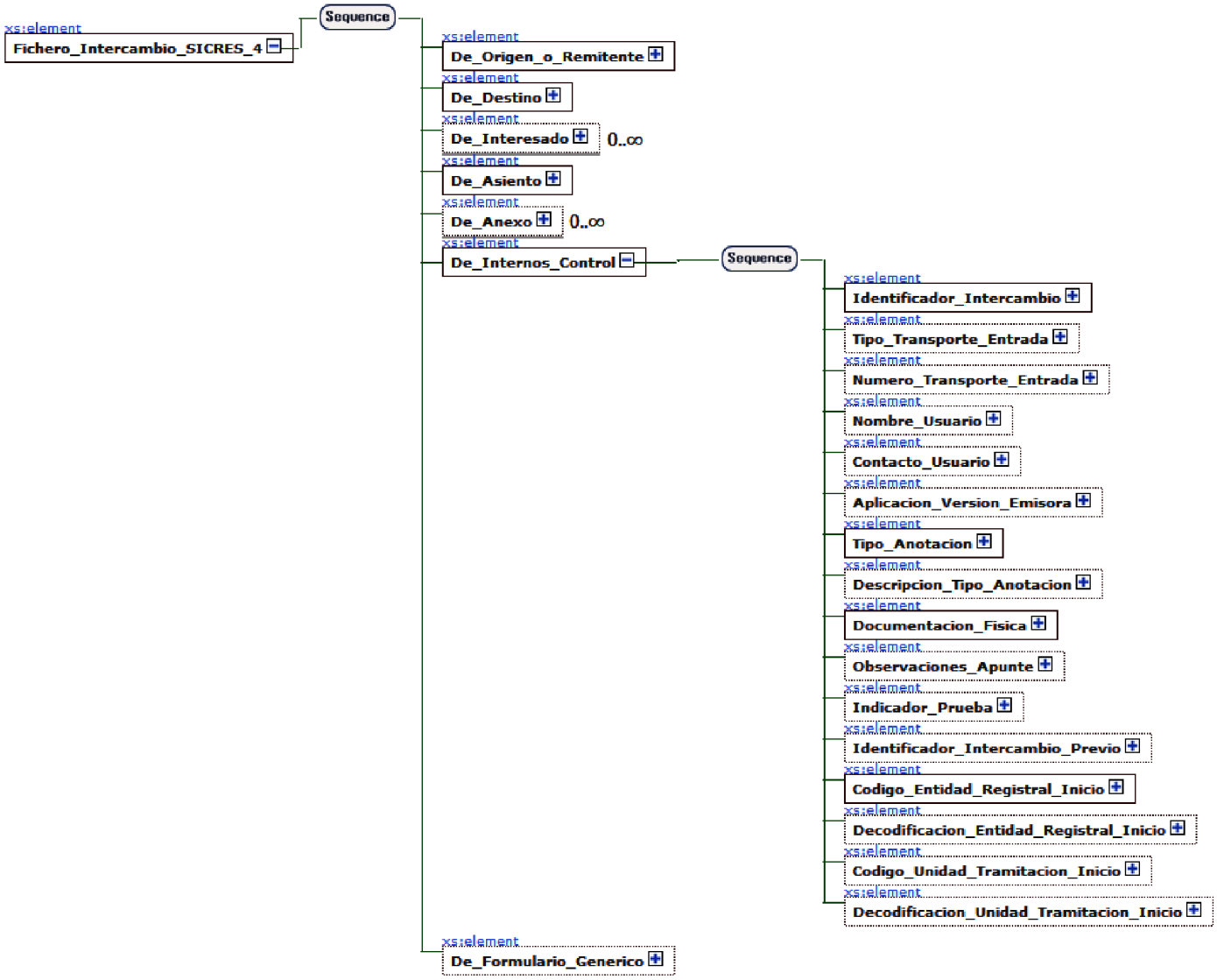


Figura 16. Esquema XML: Mensaje de datos de intercambio - Detalle de Internos y Control

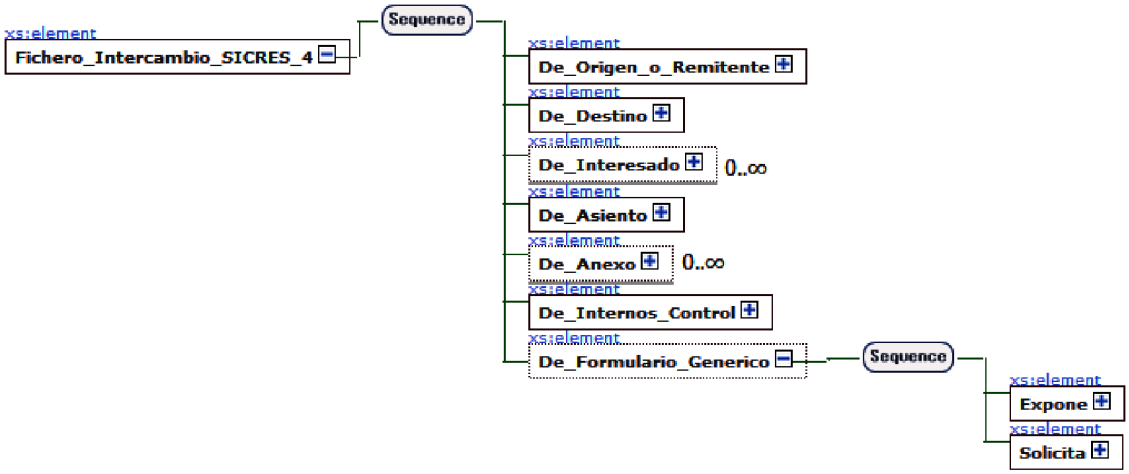


Figura 17. Esquema XML: Mensaje de datos de intercambio - Detalle de Formulario Genérico

Esquema XML del mensaje de datos de intercambio

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
	<!-- Declaracion de tipos complejos de ambito global -->
	<xs:complexType name="Datos_Persona">
		<xs:sequence>
			<xs:element name="Datos_Identificacion" minOccurs="1"
maxOccurs="1">
				<xs:complexType>
					<xs:sequence>
						<xs:element name="Tipo_Persona"
minOccurs="1" maxOccurs="1">
							<xs:simpleType>
								<xs:restriction base="xs:string">
									<xs:maxLength
value="1"/>
									<xs:enumeration
value="1"/>
									<xs:enumeration
value="2"/>
								</xs:restriction>
							</xs:simpleType>
						</xs:element>
						<xs:element
name="Tipo_Documento_Identificacion" minOccurs="1" maxOccurs="1">
							<xs:simpleType>
```

```
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="1"/>
                                            <xs:enumeration
value="N"/>
                                            <xs:enumeration
value="C"/>
                                            <xs:enumeration
value="P"/>
                                            <xs:enumeration
value="E"/>
                                            <xs:enumeration
value="X"/>
                                            <xs:enumeration
value="O"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element
name="Documento_Identificacion" minOccurs="1" maxOccurs="1">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="17"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element          name="Razon_Social"
minOccurs="0" maxOccurs="1">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="80"/>
                                        </xs:restriction>
                                    </xs:simpleType>
                                </xs:element>
                                <xs:element
name="Codigo_Directorio_Unificado" minOccurs="0" maxOccurs="1">
                                    <xs:simpleType>
                                        <xs:restriction base="xs:string">
                                            <xs:maxLength
value="21"/>
                                        </xs:restriction>
```

```
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element  name="Nombre"  minOccurs="0"
maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="30"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element          name="Primer_Apellido"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="30"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element          name="Segundo_Apellido"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="30"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                        <xs:element          name="Datos_Contacto"          minOccurs="0"
maxOccurs="1">
                            <xs:complexType>
                                <xs:sequence>
                                    <xs:element          name="Direccion_Postal"
minOccurs="0" maxOccurs="1">
                                        <xs:complexType>
                                            <xs:sequence>
                                                <xs:element  name="Pais"
minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
```

```
        <xs:restriction base="xs:string">
        <xs:maxLength value="4"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Provincia" minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="2"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Municipio" minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="5"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Direccion" minOccurs="0" maxOccurs="1">
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="160"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Codigo_Postal" minOccurs="0" maxOccurs="1">
```

```
                                                    <xs:simpleType>
        <xs:restriction base="xs:string">
        <xs:maxLength value="5"/>
        </xs:restriction>
                                                    </xs:simpleType>
                                                </xs:element>
                                            </xs:sequence>
                                        </xs:complexType>
                                    </xs:element>
                                    <xs:element
name="Direccion_Electronica_Habilitada" minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="120"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element        name="Correo_Electronico"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="160"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element            name="Telefono_Movil"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
                                                <xs:maxLength
value="20"/>
                                            </xs:restriction>
                                        </xs:simpleType>
                                    </xs:element>
                                    <xs:element              name="Telefono_Fijo"
minOccurs="0" maxOccurs="1">
                                        <xs:simpleType>
                                            <xs:restriction base="xs:string">
```

```
                                                    <xs:maxLength
value="20"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element name="Receptor_Notificaciones" type="xs:boolean"
minOccurs="0" maxOccurs="1"/>
                            <xs:element name="Canales_Notificacion" minOccurs="0"
maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="Canal_Preferente_Notificacion" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="1"/>
                                                    <xs:enumeration
value="2"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="Solicita_aviso_SMS"
type="xs:boolean" minOccurs="0" maxOccurs="1"/>
                                        <xs:element name="Solicita_aviso_correo"
type="xs:boolean" minOccurs="0" maxOccurs="1"/>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                        </xs:sequence>
                    </xs:complexType>
                    <xs:complexType name="Listado_Metadatos">
                        <xs:sequence minOccurs="1" maxOccurs="unbounded">
                            <xs:element name="Campo">
                                <xs:simpleType>
                                    <xs:restriction base="xs:string">
                                        <xs:maxLength value="80"/>
                                    </xs:restriction>
```

```
                        </xs:simpleType>
                    </xs:element>
                    <xs:element name="Valor" type="xs:string"/>
                </xs:sequence>
            </xs:complexType>
            <!-- Declaracion del elemento raiz del Mensaje de Datos de Intercambio SICRES --
>
            <xs:element name="Fichero_Intercambio_SICRES_4">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element                    name="De_Origen_o_Remitente"
minOccurs="1" maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="Codigo_Entidad_Registral_Origen" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Decodificacion_Entidad_Registral_Origen" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="120"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Unidad_Tramitacion_Origen" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
```

```
                                                </xs:element>
                                                <xs:element
name="Decodificacion_Unidad_Tramitacion_Origen" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                                <xs:restriction
base="xs:string">
                                                                        <xs:maxLength
value="120"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element        name="De_Destino"        minOccurs="1"
maxOccurs="1">
                                <xs:complexType>
                                        <xs:sequence>
                                                <xs:element
name="Codigo_Entidad_Registral_Destino" minOccurs="1" maxOccurs="1">
                                                        <xs:simpleType>
                                                                <xs:restriction
base="xs:string">
                                                                        <xs:maxLength
value="21"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Decodificacion_Entidad_Registral_Destino" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                                <xs:restriction
base="xs:string">
                                                                        <xs:maxLength
value="120"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Codigo_Unidad_Tramitacion_Destino" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                                <xs:restriction
base="xs:string">
```

```
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Decodificacion_Unidad_Tramitacion_Destino" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="120"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element      name="De_Interesado"      minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element  name="Datos_Interesado"
type="Datos_Persona" minOccurs="0" maxOccurs="1"/>
                                        <xs:element
name="Datos_Representante" type="Datos_Persona" minOccurs="0" maxOccurs="1"/>
                                        <xs:element      name="Observaciones"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element      name="De_Asiento"      minOccurs="1"
maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
```

```
                                        <xs:element      name="Modo_Registro"
minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="2"/>
                                                    <xs:enumeration
value="01"/>
                                                    <xs:enumeration
value="02"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element       name="Tipo_Registro"
minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="0"/>
                                                    <xs:enumeration
value="1"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Numero_Registro_Entrada" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="20"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element name="Resumen">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
```

```
value="240"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Fecha_Hora_Registro" minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="19"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Timestamp_Registro" type="xs:base64Binary" minOccurs="0" maxOccurs="1"/>
                                            <xs:element
name="Fecha_Hora_Presentacion" minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="19"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Timestamp_Presentacion"          type="xs:base64Binary"          minOccurs="0"
maxOccurs="1"/>
                                            <xs:element          name="Codigo_SIA"
minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="80"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Numero_Expediente" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
```

```
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Asunto_Segun_Destino" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="16"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Referencia_Externa" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="16"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Otros_Metadatos_Generales"      type="Listado_Metadatos"      minOccurs="0"
maxOccurs="1"/>
                                        <xs:element
name="Otros_Metadatos_Particulares"    type="Listado_Metadatos"    minOccurs="0"
maxOccurs="1"/>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element         name="De_Anexo"         minOccurs="0"
maxOccurs="unbounded">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element
name="Nombre_Fichero_Anexado" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
```

```
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Identificador_Fichero" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="50"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element          name="Tipo_Anexo"
minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="2"/>
                                                    <xs:enumeration
value="01"/>
                                                    <xs:enumeration
value="02"/>
                                                    <xs:enumeration
value="03"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element          name="Tipo_MIME"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element                name="Anexo"
```

```
minOccurs="0" maxOccurs="1"/>
                                        <xs:element          name="Resumen"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Formulario" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="80"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Otros_Metadatos_Generales"    type="Listado_Metadatos"    minOccurs="0"
maxOccurs="1"/>
                                        <xs:element
name="Otros_Metadatos_Particulares"   type="Listado_Metadatos"   minOccurs="0"
maxOccurs="1"/>
                                        <xs:element    name="Observaciones"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                            <xs:element  name="De_Internos_Control"  minOccurs="1"
maxOccurs="1">
                                <xs:complexType>
```

```
                                        <xs:sequence>
                                            <xs:element
name="Identificador_Intercambio" minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="33"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Tipo_Transporte_Entrada" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="2"/>
                                                        <xs:enumeration
value="01"/>
                                                        <xs:enumeration
value="02"/>
                                                        <xs:enumeration
value="03"/>
                                                        <xs:enumeration
value="04"/>
                                                        <xs:enumeration
value="05"/>
                                                        <xs:enumeration
value="06"/>
                                                        <xs:enumeration
value="07"/>
                                                        <xs:enumeration
value="08"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Numero_Transporte_Entrada" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
```

```
value="40"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element   name="Nombre_Usuario"
minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="80"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element  name="Contacto_Usuario"
minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="160"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element
name="Aplicacion_Version_Emisora" minOccurs="0" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="20"/>
                                                    </xs:restriction>
                                                </xs:simpleType>
                                            </xs:element>
                                            <xs:element     name="Tipo_Anotacion"
minOccurs="1" maxOccurs="1">
                                                <xs:simpleType>
                                                    <xs:restriction
base="xs:string">
                                                        <xs:maxLength
value="2"/>
                                                        <xs:enumeration
value="01"/>
```

```
                                                    <xs:enumeration
value="02"/>
                                                    <xs:enumeration
value="03"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Descripcion_Tipo_Anotacion" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Documentacion_Fisica" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="1"/>
                                                    <xs:enumeration
value="2"/>
                                                    <xs:enumeration
value="3"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Observaciones_Apunte" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="160"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
```

```
                                        <xs:element  name="Indicador_Prueba"
minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="1"/>
                                                    <xs:enumeration
value="0"/>
                                                    <xs:enumeration
value="1"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Identificador_Intercambio_Previo" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="33"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Codigo_Entidad_Registral_Inicio" minOccurs="1" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="21"/>
                                                </xs:restriction>
                                            </xs:simpleType>
                                        </xs:element>
                                        <xs:element
name="Decodificacion_Entidad_Registral_Inicio" minOccurs="0" maxOccurs="1">
                                            <xs:simpleType>
                                                <xs:restriction
base="xs:string">
                                                    <xs:maxLength
value="120"/>
                                                </xs:restriction>
                                            </xs:simpleType>
```

```
                                                </xs:element>
                                                <xs:element
name="Codigo_Unidad_Tramitacion_Inicio" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                                <xs:restriction
base="xs:string">
                                                                        <xs:maxLength
value="21"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                                <xs:element
name="Decodificacion_Unidad_Tramitacion_Inicio" minOccurs="0" maxOccurs="1">
                                                        <xs:simpleType>
                                                                <xs:restriction
base="xs:string">
                                                                        <xs:maxLength
value="120"/>
                                                                </xs:restriction>
                                                        </xs:simpleType>
                                                </xs:element>
                                        </xs:sequence>
                                </xs:complexType>
                        </xs:element>
                        <xs:element                 name="De_Formulario_Generico"
minOccurs="0" maxOccurs="1">
                         <xs:complexType>
                                <xs:sequence>
                                 <xs:element      minOccurs="1"      maxOccurs="1"
name="Expone">
                                        <xs:simpleType>
                                         <xs:restriction base="xs:string">
                                                <xs:maxLength value="4000"/>
                                         </xs:restriction>
                                        </xs:simpleType>
                                 </xs:element>
                                 <xs:element      minOccurs="1"      maxOccurs="1"
name="Solicita">
                                        <xs:simpleType>
                                         <xs:restriction base="xs:string">
                                                <xs:maxLength value="4000"/>
                                         </xs:restriction>
                                        </xs:simpleType>
```

```
                                    </xs:element>
                                </xs:sequence>
                            </xs:complexType>
                        </xs:element>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:schema>
```

Representación gráfica del esquema del mensaje de control

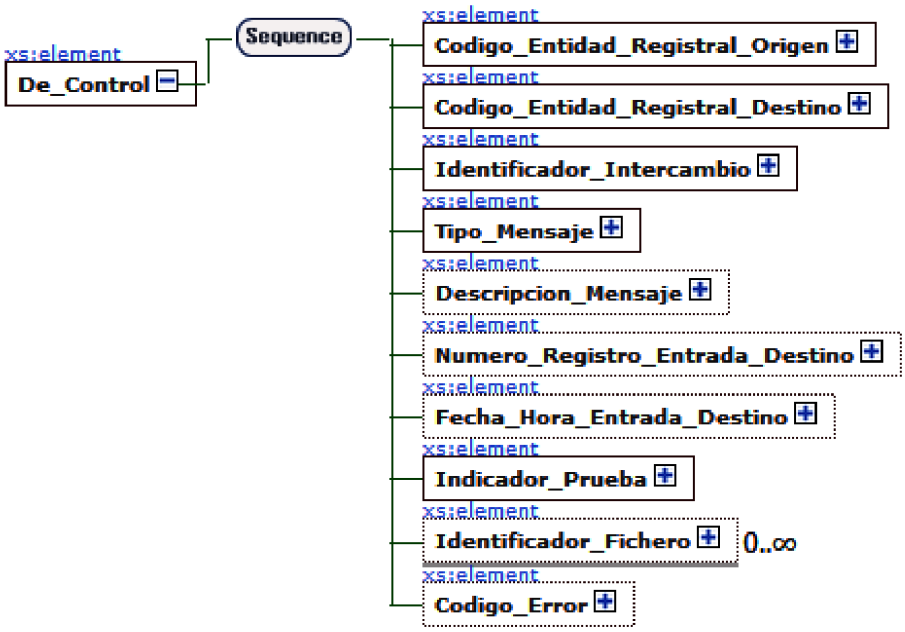


Figura 18. EsquemaXML: Mensaje de control – Visión general

Esquema XML del mensaje de control

```
<xs:schema elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
 <xs:element name="De_Control">
  <xs:complexType>
   <xs:sequence>
    <xs:element minOccurs="1" maxOccurs="1"
name="Codigo_Entidad_Registral_Origen">
     <xs:simpleType>
```

```
        <xs:restriction base="xs:string">
          <xs:maxLength value="21"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1"
name="Codigo_Entidad_Registral_Destino">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="21"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1" name="Identificador_Intercambio">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="33"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1" name="Tipo_Mensaje">
       <xs:simpleType>
        <xs:restriction base="xs:string">
                        <xs:maxLength value="2"/>
                        <xs:enumeration value="01"/>
                        <xs:enumeration value="02"/>
                        <xs:enumeration value="03"/>
                        <xs:enumeration value="04"/>
                        <xs:enumeration value="05"/>
                        <xs:enumeration value="06"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1" name="Descripcion_Mensaje">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="1024"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1"
name="Numero_Registro_Entrada_Destino">
       <xs:simpleType>
```

```
        <xs:restriction base="xs:string">
          <xs:maxLength value="20"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1"
name="Fecha_Hora_Entrada_Destino">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="19"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="1" maxOccurs="1" name="Indicador_Prueba">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="0"/>
          <xs:enumeration value="1"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="unbounded"
name="Identificador_Fichero">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="50"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
      <xs:element minOccurs="0" maxOccurs="1" name="Codigo_Error">
       <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:maxLength value="4"/>
        </xs:restriction>
       </xs:simpleType>
      </xs:element>
     </xs:sequence>
    </xs:complexType>
   </xs:element>
</xs:schema>
```

§ 38

Resolución de 19 de febrero de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Reutilización de recursos de la información

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 54, de 4 de marzo de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-2380

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público establece la regulación aplicable a la reutilización de la información elaborada o custodiada por las instancias públicas, en base a la potencialidad que le otorga el desarrollo de la sociedad de la información, el gran interés para las empresas a la hora de operar en sus ámbitos de actuación, contribuir al crecimiento económico y la creación de empleo, y para los ciudadanos como elemento de transparencia y guía para la participación democrática.

El Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal introduce en su disposición final primera dos modificaciones en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica; en primer lugar se añade un nuevo párrafo l) a la disposición adicional primera, apartado 1, del citado Real Decreto 4/2010 para añadir una Norma Técnica de Interoperabilidad sobre reutilización de recursos de información; y, en segundo lugar, se introduce una disposición adicional quinta sobre la norma técnica relativa a la reutilización de recursos de información por la cual se señala el plazo en que dicha norma deberá estar aprobada.

Las normas técnicas de interoperabilidad desarrollan aspectos concretos de diversas cuestiones, tales como: documento electrónico, digitalización, expediente electrónico, copiado auténtico y conversión, política de firma, estándares, intermediación de datos, modelos de datos, gestión de documentos electrónicos, conexión a la red de comunicaciones de las Administraciones públicas españolas, modelo de datos para el intercambio de asientos registrales y declaración de conformidad; todos ellos necesarios para asegurar los aspectos más prácticos y operativos de la interoperabilidad entre las Administraciones públicas y con el ciudadano. Estas normas técnicas de interoperabilidad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de administración electrónica, de las infraestructuras que los apoyan y de la evolución tecnológica, para dar cumplimiento al mandato del artículo 42.3 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

En particular, la Norma técnica de interoperabilidad de reutilización de recursos de información establece condiciones comunes sobre selección, identificación, descripción, formato, condiciones de uso y puesta a disposición de los documentos y recursos de

información elaborados o custodiados por el sector público, relativos a numerosos ámbitos de interés como la información social, económica, jurídica, turística, sobre empresas, educación, etc., cumpliendo plenamente con lo establecido en la citada Ley 37/2007, de 16 de noviembre.

Estas condiciones tienen el objetivo de facilitar y garantizar el proceso de reutilización de la información de carácter público procedente de las Administraciones públicas, asegurando la persistencia de la información, el uso de formatos así como los términos y condiciones de uso adecuados.

La presente norma técnica se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica y propuesta por el Comité Sectorial de Administración Electrónica.

En aplicación de lo dispuesto en el apartado 2 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, esta Secretaría de Estado resuelve:

Primero.

Se aprueba la Norma técnica de interoperabilidad de reutilización de recursos de información cuyo texto se incluye a continuación.

Segundo.

La Norma técnica de interoperabilidad de reutilización de recursos de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado», sin perjuicio de lo dispuesto en la disposición transitoria primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

NORMA TÉCNICA DE INTEROPERABILIDAD DE REUTILIZACIÓN DE RECURSOS DE INFORMACIÓN

I. Objeto

La Norma técnica de interoperabilidad de reutilización de recursos de información tiene por objeto establecer el conjunto de pautas básicas para la reutilización de documentos y recursos de información elaborados o custodiados por el sector público a los que se refiere el artículo 3 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público por cualquier agente interesado.

II. Ámbito de aplicación

Esta norma será de aplicación para la puesta a disposición, para su reutilización, de recursos de información de carácter público por parte de cualquier órgano de la Administración pública o Entidad de Derecho Público vinculada o dependiente de aquella en el ámbito establecido en el artículo 3 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

A los efectos de esta norma, las definiciones, palabras, expresiones y términos se entenderán en el sentido indicado en el glosario incluido en el anexo I.

III. Selección de la información reutilizable

1. Al objeto de seleccionar los documentos y recursos de información aptos para la reutilización, se considerarán prioritarios los de mayor relevancia y potencial social y económico.

2. Los documentos y recursos de información reutilizables serán primarios, evitando las modificaciones o alteraciones de la información existente en la fuente, al objeto de evitar errores que se puedan producir durante la manipulación de la información.

3. El nivel granular será el más fino posible, evitando agregaciones adicionales, para posibilitar una reutilización adecuada a cualquier necesidad.

4. Los documentos y recursos de información reutilizables tendrán asociada información estructurada que permita su procesamiento automatizado.

5. Los documentos y recursos de información de elaboración o recogida periódica puestos a disposición para su reutilización estarán actualizados a sus últimas versiones y se indicará la fecha de última actualización, así como el periodo de la misma.

IV. Identificación de la información reutilizable

1. Los documentos y recursos de información reutilizables estarán identificados mediante referencias únicas y unívocas, basadas en identificadores de recursos uniformes, que componen la base necesaria para habilitar un mecanismo coherente de reutilización de la información a través de Internet. Con el uso de estos identificadores se podrá hacer referencia a los documentos o recursos que representan de forma unívoca, estable, extensible, persistente en el tiempo y ofreciendo garantías de procedencia, requisitos clave para facilitar su posterior reutilización.

2. Para la construcción de los identificadores de recursos uniformes se tendrán en cuenta los siguientes requisitos:

a) Se usarán los protocolos HTTP o HTTPS, con el fin de garantizar el direccionamiento y resolución de cualquier identificador de los recursos en la web.

b) Dado que pueden existir representaciones distintas asociadas a un mismo recurso de información, un servidor al que se le solicita un identificador de recurso uniforme debería gestionar dicha petición en función de la cabecera HTTP recibida, devolviendo la representación del recurso adecuada a las preferencias del cliente.

c) Para la composición de los identificadores de recursos uniformes se usará un esquema consistente, extensible y persistente, preferentemente de acuerdo con el esquema definido en el anexo II. Las normas de construcción de los mismos seguirán unos patrones determinados que ofrezcan coherencia en la uniformidad, los cuales podrán ser ampliados o adaptados en caso de necesidad. Aquellos Identificadores que sean creados y publicados en algún momento, deberán mantenerse en el tiempo.

d) Los identificadores de recursos uniformes seguirán una estructura de composición comprensible y significativa. El identificador deberá ofrecer información de manera que pueda ser entendido y fácilmente escrito por personas lo que permitirá disponer de información sobre el propio recurso, así como su procedencia únicamente interpretando el identificador.

e) El identificador de recursos uniforme que identifica cada documento o recurso, en la medida de lo posible, no revelará información sobre la implementación técnica de generación del recurso representado.

V. Descripción de la información reutilizable

1. Para la descripción de los documentos y recursos de información reutilizables puestos a disposición pública se asociarán los metadatos mínimos recogidos en el anexo III; para los valores de ciertos metadatos se tendrá en cuenta lo establecido en los anexos IV y V.

2. Cada distribución tendrá asociados, al menos, los metadatos recogidos en el anexo III.

3. Para facilitar la reutilización de vocabularios se utilizará el Centro de Interoperabilidad Semántica de la Administración previsto en el artículo 10, apartado 3 del Real Decreto 4/2010, dichos vocabularios se publicarán de acuerdo con las condiciones de formato establecidas en el apartado VI.

VI. Formato de los documentos y recursos de información reutilizables

1. Con el objeto de garantizar la independencia en la elección de alternativas tecnológicas por los ciudadanos y las Administraciones públicas y la adaptabilidad al progreso de la tecnología, los documentos y recursos de información reutilizables puestos a disposición pública, los metadatos y los servicios asociados a los mismos utilizarán estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean

de uso generalizado por la ciudadanía, siendo de aplicación lo previsto en el artículo 11 del Real Decreto 4/2010, de 8 de enero y se ceñirán a lo establecido en la Norma técnica de interoperabilidad de catálogo de estándares, aprobada por Resolución de 3 de octubre de 2012, de la Secretaría de Estado de Administraciones Públicas.

2. Se podrán utilizar otros estándares cuando existan particularidades que lo justifiquen, cuando no sea viable la conversión a un estándar más adecuado o, bien no exista alternativa, siendo de aplicación lo previsto sobre estándares en el artículo 11 del Real Decreto 4/2010, de 8 de enero.

3. Cualquier documento o recurso de información reutilizable podrá ser puesto a disposición pública a través de una o varias distribuciones en varios formatos distintos, con el objeto de facilitar la reutilización a agentes con distintos perfiles.

4. Se seleccionarán preferentemente formatos que ofrezcan representación semántica de la información, con el fin de facilitar una mejor comprensión de la información representada y su tratamiento automatizado. Si los formatos elegidos lo permiten, se priorizará el uso de esquemas o vocabularios internacionalmente reconocidos para representar la información.

5. Se incluirá preferentemente información de ayuda complementaria sobre los esquemas o vocabularios utilizados para representar la información.

VII. Términos y condiciones de uso aplicables

1. Las condiciones de reutilización específica de los órganos y entidades de Derecho Público de las Administraciones públicas se ajustarán a lo dispuesto en la Ley 37/2007, de 16 de noviembre, y su normativa de desarrollo. Lo establecido en el artículo 8 del Real Decreto 1495/2011, de 24 de octubre, podrá ser utilizado como referencia por otras Administraciones Públicas.

2. Dichas condiciones de reutilización globales a un organismo, disponibles en formato digital y procesables electrónicamente, podrán ser complementadas por condiciones específicas aplicadas a categorías de documentos o recursos de información concretos mediante licencias-tipo, disponibles en las mismas condiciones que las globales.

VIII. Puesta a disposición de los documentos y recursos de información

1. Los documentos o recursos de información puestos a disposición públicamente atenderán al principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente, según lo establecido en el artículo 4.c) de la Ley 11/2007, de 22 de junio.

2. Cada órgano, organismo o entidad de derecho público del ámbito establecido en el artículo 1.2 del Real Decreto 1495/2011, de 11 de octubre, proporcionará información estructurada sobre los documentos y recursos de información susceptibles de reutilización, preferentemente a través de un espacio dedicado en su sede electrónica con el Localizador de Recurso Uniforme correspondiente, según el modelo http://www.sede.gob.es/datosabiertos. El resto de los órganos y entidades de derecho público de las Administraciones públicas seguirá sus normas reguladoras específicas.

3. Se asociará a los documentos o recursos de información reutilizables puestos a disposición pública la información necesaria que permita su interpretación.

4. En el caso de que se realice una puesta a disposición de la información mediante puntos de acceso dinámico, complementarios a los puntos de descarga masiva, se elaborará un documento técnico explicativo sobre el uso y configuración de estos puntos de acceso con, al menos, los parámetros de consulta permitidos, el tipo de información devuelta y los formatos aceptados.

5. Las direcciones electrónicas que alberguen documentos, recursos de información o catálogos de información pública susceptibles de reutilización contendrán información de aviso de dicha condición.

IX. Catálogo de información pública reutilizable

1. A efectos de la colaboración de los distintos órganos y entidades, los catálogos de información pública reutilizable implementarán:

a) Una interfaz de publicación, que permita a los diferentes órganos y entidades públicos poner a disposición los metadatos de sus documentos y recursos de información reutilizables.

b) Una interfaz de consulta, que permita que las aplicaciones de terceros puedan acceder a funcionalidades de búsqueda.

2. La descripción de cada categoría de documentos o recursos de información se realizará en fichas donde se recogerán, al menos, los metadatos obligatorios, descritos en el anexo III. Para la definición de catálogos y registros se podrá aplicar el modelo de plantilla incluido en el anexo VI.

3. Se proporcionará acceso al contenido del catálogo de dos formas:

a) Mediante documentos HTML legibles para las personas.

b) Mediante información procesable automáticamente que permita la reutilización de los propios metadatos del catálogo y la interoperabilidad con otros catálogos. El propio catálogo se ofrecerá como un conjunto de datos reutilizable, utilizando para ello el vocabulario internacionalmente reconocido DCAT.

ANEXO I

Glosario

Agente reutilizador: persona, física o jurídica que reutilice información del sector público, ya sea para fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública.

Dato: Una representación de hechos, conceptos o instrucciones de un modo formalizado, y adecuado para comunicación, interpretación o procesamiento por medios automáticos o humanos.

Distribución: Información en un formato concreto, accesible desde un URL concreto. Un recurso de información puede disponer de una o múltiples distribuciones.

Documento: Toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos.

Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Documentos o recursos de información reutilizable: Documentos que obran en poder de las Administraciones, órganos y entidades de Derecho Público del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública, de acuerdo con el ámbito de aplicación y exclusiones establecidos en el artículo 3 de la Ley 37/2007, de 16 de noviembre.

Documento o recurso de información primario: Dato tal y como se capta de la fuente sin modificaciones o alteraciones.

Extensiones multipropósito de correo de Internet (Multipurpose Internet Mail Extensions): Serie de convenciones o especificaciones dirigidas al intercambio, a través de Internet, de todo tipo de ficheros –texto, audio, vídeo, u otros– de forma transparente para el usuario.

Formato: Conjunto de características técnicas y de presentación de un recurso de información o documento.

Identificador de Recursos Uniforme: Cadena alfanumérica compacta que identifica recursos –físicos o abstractos– en la web de forma unívoca. La diferencia respecto a un Localizador de Recursos Uniforme es su invariabilidad en la referencia de recursos.

Infraestructura de Descripción de Recursos: Marco para la descripción semántica de recursos en la web, de manera que se dota de sentido a las representaciones en la web para que los datos puedan ser procesables automáticamente. RDF no es un formato, sino que existen distintas formas de representación –XML, N3, Turtle, etc.

Interfaz de Programación de Aplicaciones: Punto de comunicación entre componentes de software, que ofrece un conjunto de llamadas a librerías de programación que ofrecen acceso a servicios desde los procesos, consiguiendo la abstracción en la programación entre niveles inferiores y superiores del software.

Linked Open Data: Aproximación de ciertas iniciativas de apertura de datos (Open Data) basada en tecnologías de la Web Semántica, donde se relacionan datos definidos de forma semántica y que están identificados y representados en la web.

Localizador de Recursos Uniforme: Término usado para denominar ciertos identificadores de recursos uniformes cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo.

Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

Nivel de granularidad: Es el nivel de detalle de los datos, en la medida en la que trata el nivel más atómico por el cual se definen los datos.

Ontología: Descripción formal de los conceptos y relaciones que pueden existir sobre agentes o una comunidad. Especificación consensuada que describe un dominio de información.

Open Data: Iniciativa de apertura de datos aptos para su reutilización por parte de terceros.

Punto de acceso dinámico: Servicio de consulta que permite obtener información estructurada a través de peticiones basadas en parámetros configurables.

RDFa: Forma de representación de datos estructurados presentes en documentos web mediante anotaciones semánticas (RDF), incluidas en el código e invisibles para el usuario, que permiten a las aplicaciones interpretar esta información y utilizarla de forma eficaz.

SPARQL (SPARQL Protocol and RDF Query Language): Tecnología de consulta de información sobre diversas fuentes de datos que almacenan los mismos siguiendo el modelo de descripción RDF.

Tripleta RDF: Sentencia en la que se describe la relación de un recurso con otro a través de un sujeto, un predicado (o propiedad), y un objeto.

W3C (World Wide Web Consortium): Consorcio neutro internacional de reconocido prestigio donde las organizaciones Miembro, el personal a tiempo completo y el público en general, trabajan conjuntamente para desarrollar estándares para la web.

Web Semántica: infraestructura de tecnologías y mecanismos que ofrece la posibilidad de definir, integrar, compartir y reutilizar información en la web entre distintas partes de forma automatizada en función de su significado.

Acrónimos y abreviaturas

API: Application Programming Interface (Interfaz de Programación de Aplicaciones).

DCAT: Data Catalog Vocabulary (Vocabulario de Catálogo de Datos).

HTTP: Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto).

HTTPS: HTTP Secure (Protocolo de Transferencia de Hipertexto Seguro).

MIME: Multipurpose Internet Mail Extensions (Extensiones multipropósito de correo de Internet).

OWL: Web Ontology Language (Lenguaje de Ontologías Web).

RDF: Resource Description Framework (Infraestructura de Descripción de Recursos).

RDF-S: RDF Schema (Esquema para la Infraestructura de Descripción de Recursos).

RSS: RDF Site Summary (Resumen del Sitio en RDF) o Really Simple Syndication (Sindicación Realmente Simple).

SKOS: Simple Knowledge Organization System (Sistema de Organización del Conocimiento Simple).

URI: Uniform Resource Identifier (Identificador de Recurso Uniforme).

URL: Uniform Resource Locator (Localizador de Recurso Uniforme).

WWW: World Wide Web.

ANEXO II

Esquema de URI

El esquema de identificadores de recursos uniformes o URI establece un mecanismo de identificación común para los datos que se exponen públicamente, de forma que se pueda hacer referencia a estos de forma única, fiable y persistente en el tiempo, requisito clave para facilitar su posterior reutilización.

Características básicas del esquema a implementar

Los requisitos genéricos para diseñar el esquema de URI son los siguientes:

a) Utilizar el protocolo HTTP, de forma que se garantiza la resolución de cualquier URI en la web.

b) Usar una estructura de composición de URI consistente, extensible y persistente. Las normas de construcción de los URI seguirán unos patrones determinados que ofrezcan coherencia en la uniformidad, los cuales podrán ser ampliados o adaptados en caso de necesidad.

c) Los URI seguirán una estructura de composición comprensible y relevante. Esto significa que el propio identificador debe ofrecer información semántica autocontenida, lo que permitirá a cualquier agente reutilizador disponer de información sobre el propio recurso, así como su procedencia.

d) No se debe exponer información sobre la implementación técnica de los recursos que representan los URI. En la medida de lo posible se omitirá información específica sobre la tecnología subyacente del recurso representado; por ejemplo, no se incluirán las extensiones correspondientes a tecnologías con las que se generan los recursos web como.php,.jsp, etc.

e) Los URI deben cumplir el principio de persistencia, lo que significa que los que ya han sido creados previamente nunca deberían variar, y que el contenido al que hacen referencia, debería ser accesible. En el caso de que sea necesario cambiar o eliminar el recurso al que apunta un identificador, se deberá establecer un mecanismo de información sobre el estado del recurso usando los códigos de estado de HTTP. En el caso de poder ofrecer una redirección a la nueva ubicación del recurso, se utilizarán los códigos de estado HTTP 3XX, mientras que para indicar que un recurso ha desaparecido permanentemente se utilizará el código de estado HTTP 410.

Estructura básica de los URI

Todos los URI tendrán una estructura uniforme que ofrecerá coherencia al sistema de representación de los recursos, cubrirá los principios básicos de construcción de las mismas y contendrá información intuitiva sobre la procedencia y el tipo de información que identifica.

La base de los URI incluirá información básica sobre la procedencia de los datos, que representará un espacio dedicado por parte de la entidad para albergar su plataforma de reutilización; para indicar la situación de la información relativa a la iniciativa de datos abiertos –portal web, catálogo, u otra información sobre el proyecto– se utilizará preferentemente www.sede.gob.es/datosabiertos o bien http://organismo.gob.es/datosabiertos cuando los recursos no se ubiquen en una sede electrónica. El resto de los recursos semánticos podrán seguir un patrón dependiente únicamente del dominio (http://organismo.gob.es).

Para el caso de los URI de la documentación en los portales web de los organismos, cabe en su caso determinar primero el idioma, según la norma internacional correspondiente ISO 639-1, y después el canal, según el modelo http://organismo.gob.es/idioma/datosabiertos, por ejemplo http://organismo.gob.es/es-ES/datosabiertos. Esto dependerá de las políticas y de las características tecnológicas de cada organismo. Esto no será necesario en la gestión de recursos semánticos, ya que su propia descripción admite varios idiomas para el mismo recurso con un URI único.

Los elementos que componen la ruta de un URI son: sector, carácter de la información, tipo de representación, dominio o temática y los conceptos específicos. Dentro de la composición de una URI se especifican por el siguiente orden:

http://{base}/{carácter}[/{sector}][/{dominio}][/{concepto}][.{ext}]

O, alternativamente, utilizando los identificadores de fragmento mediante la marca «#» al final de la dirección:

http://{base}/{carácter}[/{sector}][/{dominio}][.{ext}][#{concepto}]

Esta estructura general de un URI puede variar dependiendo de las necesidades o preferencias de una organización, siendo obligatorio mantener invariables los elementos base y carácter. La parte final del URI, podría identificar la temática general o específica del recurso, el concepto concreto que representa y/o el formato de representación mediante una extensión. Estos dos últimos componentes son opcionales dependiendo del tipo de información que represente.

Carácter:

Valor	Información que representa
Catálogo.	Documento o recurso de información incluido en el catálogo, con una lista de recursos o entidades de un mismo dominio. Habitualmente estos documentos y recursos de información contendrían datos comunes como condiciones de uso, origen, vocabularios utilizados, etc. También identifica al catálogo en sí.
Def.	Vocabulario u ontología utilizada como modelo semántico. Habitualmente esquemas RDF-S u ontologías representadas mediante OWL.
Kos.	Sistema de organización del conocimiento sobre un dominio concreto. Habitualmente taxonomías, diccionarios o tesauros, representados mediante SKOS.
Recurso.	Identificación abstracta única y unívoca de un recurso u objeto físico o conceptual. Estos recursos son las representaciones atómicas de los documentos y recursos de información y suelen ser instancias de los conceptos que se definen en los vocabularios. Si se especifica extensión (o formato) en el URI indica que es la representación del recurso. Pueden existir dos tipos de representaciones de un recurso básicas: un documento legible para humanos –normalmente HTML– o para las máquinas, en cualquiera de los formatos de representación de RDF. El tipo concreto del documento será especificado mediante extensiones del propio documento.

Sector:

La selección de un sector adecuado, acompañado del dominio específico del origen, le dará a cualquier usuario la confianza de conocer el tipo de información que está manejando y la fuente de la misma. Se seleccionará un identificador del sector (primario), según lo especificado en el anexo IV. Cada documento o recurso de información, vocabulario o esquema de conceptos debe pertenecer a un único sector. Si pertenece a más de uno, se utilizará el más representativo o alguno que se pueda considerar común.

Dominio o temática de la información:

Para identificar los elementos específicos dentro de un sector –recursos de información, vocabularios, esquemas de conceptos, etc.–, se creará una referencia adecuada que represente al dominio o temática de la información tratada.

Conceptos específicos:

Los últimos elementos de ciertos URI –tras el carácter, sector y nombre del dominio de la información– incluyen a los conceptos e instancias específicas de recursos. Los conceptos son representaciones abstractas que se corresponden con las clases o propiedades de los vocabularios u ontologías utilizados para representar semánticamente los recursos. Además del concepto, se podrá representar una referencia unívoca a instancias concretas. También se podrán representar esquemas de conceptos abstractos, dentro de sistemas de gestión del conocimiento (taxonomías, tesauros, etc.).

Formato:

Dado que los documentos que representan recursos pueden ser de diversos tipos, éstos se identificarán a través de la extensión del propio fichero, como, por ejemplo, «doc.html», «doc.rdf» o «doc.n3». Para la identificación de los recursos de forma abstracta se omitirá la extensión.

A continuación, se especifican los tipos de URI específicos para recursos semánticos de una iniciativa basada en Linked Data.

URI para identificar catálogos y conjuntos de datos

Si la iniciativa de reutilización sólo dispone de un catálogo, se podría representar a través del URI: http://{base}/catalogo

En el caso de que el organismo disponga de más de un catálogo se definirá una referencia descriptiva para cada catálogo que haga referencia al tema o dominio del mismo. Para ello se utilizará el URI: http://{base}/catalogo/{sector}

Los conjuntos de datos incluidos en cada catálogo se identifican mediante un URI con un identificador único para cada conjunto de datos: http://{base}/catalogo/{dataset}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/catalogo#{dataset}

URI para identificar vocabularios

Cualquier vocabulario u ontología seguirá el esquema: http://{base}/def/{sector}/{dominio}

Donde sector indicará el tema del vocabulario y dominio corresponderá a la referencia asignada al vocabulario, una representación textual breve pero descriptiva.

Las clases y propiedades del vocabulario tendrán como base el URI correspondiente al vocabulario donde se definen, compuesto con los identificadores de las clases o propiedades según el esquema: http://{base}/def/{sector}/{dominio}/{propiedad|Clase}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/def/{sector}/{dominio}#{propiedad|Clase}

URI para identificar esquemas de conceptos

Cualquier sistema de organización del conocimiento –taxonomías, diccionarios, tesauros, etc.– sobre un dominio concreto será identificado mediante un esquema de URI basado en la estructura: http://{base}/kos/{sector}/{dominio}

Donde sector indicará el tema del esquema de conceptos y dominio corresponderá a la referencia asignada a dicho esquema de clasificación. Ésta referencia del dominio será una breve representación textual pero descriptiva.

Los conceptos incluidos en el esquema tendrán como base el URI correspondiente al esquema donde se definen y tendrán la forma: http://{base}/kos/{sector}/{dominio}/{Concepto}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/kos/{sector}/{dominio}#{Concepto}

URI para identificar a cualquier instancia física o conceptual

Estos recursos son las representaciones atómicas de los documentos y recursos de información. A su vez suelen ser instancias de las clases que se definen en los vocabularios. Estos recursos se identifican mediante el esquema: http://{base}/recurso/{sector}[/{dominio}]/{clase}/{ID}

O, en su defecto, utilizando la nomenclatura de identificadores de fragmentos (#): http://{base}/recurso/{sector}[/{dominio}]/{clase}#{ID}

Donde sector indicará el tema relacionado con el recurso y clase corresponderá al tipo de concepto que describe al recurso. Habitualmente coincide con el identificador de una de las clases que caracteriza al recurso. El ID es un identificador que permite distinguir al recurso entre el resto de las instancias del mismo tipo, dentro del sistema. El dominio, relativo al recurso, podría corresponder al especificado en el propio vocabulario que define las clases de la instancia, es opcional.

Normalización de los componentes de los URI

Para garantizar la coherencia y el mantenimiento posterior del esquema de URI se aplicarán las siguientes reglas para normalizar las distintas partes que componen los URI:

a) Seleccionar identificadores alfanuméricos cortos únicos, que sean representativos, intuitivos y semánticos.

b) Usar siempre minúsculas, salvo en los casos en los que se utilice el nombre de la clase o concepto. Habitualmente, los nombres de las clases se representan con el primer carácter de cada palabra en mayúsculas.

c) Eliminar todos los acentos, diéresis y símbolos de puntuación. Como excepción puede usarse el guión (–).

d) Eliminar conjunciones y artículos en los casos de que el concepto a representar contenga más de una palabra.

e) Puede usarse el guión (–) como separador entre palabras.

f) Evitar en la medida de lo posible la abreviatura de palabras, salvo que la abreviatura sea intuitiva.

Los términos que componen los URI deberán ser legibles e interpretables por el mayor número de personas posible, por lo que se utilizará el castellano o cualquiera de las lenguas oficiales.

Prácticas relativas a la gestión de recursos semánticos a través de URI

Se aplicarán las prácticas siguientes para la gestión de recursos semánticos descritos en RDF:

a) Siempre que sea posible, y existan versiones del recurso en formato legible para personas HTML o similar y RDF, el servidor que gestiona los URI realizará negociación del contenido en función de la cabecera del agente que realiza la petición. En el caso de que el cliente acepte un formato de representación RDF en cualquiera de sus notaciones (p.e., especificando en su cabecera que acepta el tipo MIME application/rdf+xml) se servirá el documento RDF a través del mecanismo de redirecciones alternativas mediante los códigos de estado HTTP 3XX. De la misma forma, si es posible, se servirá la representación en cualquier otro formato preferido por el cliente.

b) En el caso de que no se realice una negociación del contenido desde el servidor y, para favorecer el descubrimiento de contenido RDF desde los documentos HTML relacionados con las descripciones de los recursos, se incluirán enlaces a la representación alternativa en cualquiera de las representaciones en RDF desde los propios documentos HTML de la forma <link rel=«alternate» type=«application/rdf+xml» href=«documento.rdf»> o similar. En esa sentencia se incluye el tipo de formato MIME del documento (application/rdf +xml, text/n3, etc.).

c) Cuando se establezcan enlaces entre distintos recursos de información, se procurará la generación de enlaces que conecten los recursos bidireccionales para facilitar la navegación sobre los recursos de información en ambos sentidos.

ANEXO III

Metadatos de documentos y recursos de información del catálogo

A continuación se describen los distintos metadatos asociados con el catálogo y los documentos y recursos de información incluidos en él, además del término recomendado para su representación usando vocabularios estándar que se identifican por las abreviaturas de su espacio de nombres. Además de la denominación, descripción del metadato y el tipo de dato que se deberá usar para la representación, se especifica si es obligatorio –columna R (requerido)– y si admite más de un metadato de ese tipo –columna M (múltiple), como podría ser en el caso de las descripciones en distintos idiomas.

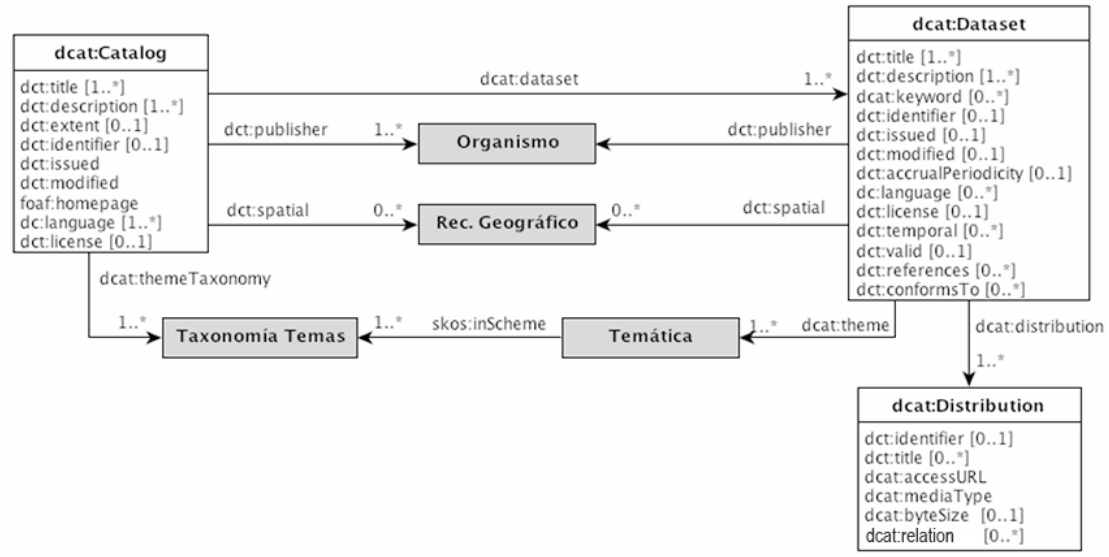
Para la descripción y exposición de los metadatos recogidos en este anexo se usarán los vocabularios y esquemas de valores propuestos, mediante tecnologías de la Web Semántica –al menos, la descripción de recursos en RDF en cualquiera de sus formatos de representación–, al objeto de facilitar la interoperabilidad a nivel semántico de los sistemas que compartan esta representación estándar.

Vocabularios:

Vocabulario	URI
XML Schema	xsd: http://www.w3.org/2001/XMLSchema#
Simple Knowledge Organization System (SKOS)	skos: http://www.w3.org/2004/02/skos/core#
Dataset Catalog (dcat)	dcat: http://www.w3.org/ns/dcat#
Dublin Core Terms	dct: http://purl.org/dc/terms/
Dublin Core Elements	dc: http://purl.org/dc/elements/1.1/
W3C Time Ontology	time: http://www.w3.org/2006/time#
Friend Of A Friend (FOAF)	foaf: http://xmlns.com/foaf/0.1/

La representación semántica se basa en el vocabulario DCAT, desarrollado por la entidad World Wide Web Consortium (W3C) y que permite la estandarización en la definición de catálogos de documentos y recursos de información. Un catálogo de documentos y recursos de información se representa mediante instancias de tipo dcat:Catalog e incluye una colección de (dcat:Dataset). Estas instancias tienen propiedades que hacen referencia a otros recursos y conceptos semánticos identificados en los anexos del presente documento y que son representados gráficamente en el siguiente diagrama y detalladas a continuación. Las entidades o propiedades básicas que se detallan en este anexo podrán ser enriquecidas con metadatos adicionales que se estimen oportunos para la mejora de la calidad de la información.

Al menos, los recursos que representen al catálogo de datos y a sus conjuntos de datos deberán ser identificado mediante un URI específico que siga el esquema de definido en el anexo II.



Catálogo (dominio dcat: Catalog)					
Metadato	**Descripción**	**propiedad**	**R**	**M**	**Tipo y Esquema de valores**
Nombre	Breve título o nombre dado al catálogo de datos.	dct:title	✓	✓	Literal. Cadena alfanumérica (se recomienda en varios idiomas).
Descripción	Resumen descriptivo del catálogo de datos.	dct:description	✓	✓	Literal. Cadena alfanumérica (se recomienda en varios idiomas).
Órgano publicador	Entidad que publica el catálogo.	dct:publisher	✓	–	foaf:Agent. Se especificará el URI correspondiente a un órgano público diferenciados por un código alfanumérico único para cada órgano/unidad/oficina, que será extraído del Directorio Común gestionado por el MINHAP según el esquema siguiente: http://datos.gob.es/recurso/sector- publico/org/ Organismol(ID- MINHAP}
Tamaño del catálogo	Número total de documentos y recursos de información inventariados en el catálogo.	dct:extent	–	–	dct:SizeOrDuration. Se recomienda incluir el valor de un número entero y su representación textual equivalente.
Identificador	Referencia para identificar el catálogo.	dct:identifier	–	–	xsd:anyURI. URI que identifica la descripción actual del catálogo.
Fecha de creación	Fecha de publicación inicial del catálogo	dct:issued	✓	–	Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD.
Fecha de actualización	Fecha en la que se modificó por última vez el catálogo (se añade, elimina o modifica un documento o recurso de información).	dct:modified	✓	–	Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD.
Idioma(s)	Idioma(s) en el(los) que se proporciona la información del catálogo.	dc:language	✓	✓	Literal. Valores normalizados de etiquetas para identificar idiomas definidos en el RFC 5646 («es», «ga», «ca», «eu», «en», «fr»}. Se usará una etiqueta por cada propiedad.

Catálogo (dominio dcat: Catalog)					
Metadato	**Descripción**	**propiedad**	**R**	**M**	**Tipo y Esquema de valores**
Cobertura geográfica	Ámbito geográfico cubierto por el catálogo.	dct:spatial	–	✓	Recurso. Se aplicará preferentemente lo establecido al respecto en el anexo V. Un recurso por propiedad.
Temáticas	Totalidad de materias incluidas en el catálogo.	dcat:themeTaxo-nomy	✓	✓	skos:ConceptScheme. Se aplicará preferentemente la taxonomía definida en el anexo IV. Su valor es: http://datos.gob.es/kos/sector-publico/sector/
Página web	Dirección web de acceso al catálogo de datos (acceso para el público).	foaf:homepage	✓	–	Recurso. URI que referencia a la portada del catálogo.
Términos de uso	Referencia a los términos de uso generales del catálogo.	dct:license	✓	–	Recurso. URI que referencia al recurso que describe los términos de uso.
Documento(s) y recurso(s) de información	Lista de cada uno de los documentos y recursos de información del catálogo.	dcat:dataset	✓	✓	dcat:Dataset. Tendrá tantas propiedades como entradas en el catálogo. (Ver metadatos de documentos y recursos de información).

Documento y recurso de información (dominio dcat: Dataset)					
Metadato	**Descripción**	**propiedad**	**R**	**M**	**Tipo y Esquema de valores**
Nombre	Nombre o título del documento o recurso de información.	dct: title	✓	✓	Literal. Cadena alfanumérica (se recomienda en varios idiomas).
Descripción	Descripción detallada del documento o recurso de información.	dct :description	✓	✓	Literal. Cadena alfanumérica (se recomienda en varios idiomas).
Temática(s)	Temática o materia primaria del documento o recurso de información.	dcat: theme	✓	✓	skos:Concept. Se recomienda hacer referencia a un tema asociado con el sector público, según la taxonomía definida en el anexo IV.
Etiqueta(s)	Etiqueta(s) textual(es) que permiten categorizar libremente el documento o recurso de información.	dcat:keyword	–	✓	Literal. Cadena alfanumérica compacta. Pueden incluirse varias propiedades (una por etiqueta).
Identificador	URI que identifica al documento o recurso de información.	det:identifie	–	–	xsd:anyURI. URI que identifica la ficha descriptiva del documento o recurso de información.
Fecha de creación	Fecha de creación del documento o recurso de información.	dct : issued	–	–	Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD.
Fecha de última actualización	Última fecha conocida en la que se modificó o actualizó el contenido del documento o recurso de información.	det:modified	–	–	Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD.
Frecuencia de actualización	Periodo de tiempo aproximado transcurrido entre actualizaciones del documento o recurso de información, si hubiera	dct : accrualPeriodicity	–	–	dct:Frequency. Se recomienda especificar periodos normalizados con formato ISO-8601 (PT), o similar.
Idioma(s)	Idioma(s) en el(los) que se encuentra la información del documento o recurso de información.	dc:language	–	✓	Literal. Valores normalizados de etiquetas para identificar idiomas definidos en el RFC 5646 («es», «ga», «ca», «eu», «en», «fr»}. Se usará una etiqueta por propiedad.
Organismo que expone y publica los datos	Organismo que publica el documento o recurso de información.	dct:publisher	✓	–	foaf:Agent. Se especificará el URI correspondiente a un organismo público diferenciados por un código alfanumérico único para cada órgano/ unidad/oficina, que será extraído del Directorio Común gestionado por el MINHAP según el esquema siguiente: http:lldatos.gob.es/recu rso/sector-publico/org/Organismo){ID-MINHAP }
Condiciones de uso	Recurso que describe las condiciones de uso o licencia específica aplicable al propio documento o recurso de información.	dct : license	–	–	dct:LicenseDocument o similar. Se especificará un URI que referencia al recurso que define las condiciones de uso. Si no es una licencia-tipo, y si fuese necesario, en la descripción se podría indicar contraprestación económica utilizando valores del código de divisa normalizado por el estándar ISO-4217 (EUR, USD, GBP, etc.).
Cobertura geográfica	Ámbito geográfico cubierto por el documento o recurso de información.	dct:spatial	–	✓	Recurso. Puede tomar uno de los valores que representan las provincias españolas, según se expresan en el anexo V.
Cobertura temporal	Fecha de inicio, fin y la duración del periodo cubierto por el documento o recurso de información.	dct: temporal	–	✓	dct:PeriodOfTime. Periodo de tiempo que puede ser definido mediante la ontología de Tiempo del W3C (time:)
Vigencia del recurso	Fecha de validez de un documento o recurso de información o en la que se estima una modificación o actualización de su contenido.	dct:valid	–	–	Literal. Fecha/Hora con formato ISO-8601: YYYY-MM-DDThh:mm:ssTZD.
Recurso(s) relacionado(s)	Enlaces a recursos relacionados con el documento o recurso de información (información sobre los propios datos, material audiovisual, etc.).	dct : references	–	✓	Recurso. URI que identifica al recurso relacionado. Se pueden incluir tantas propiedades como referencias se conozcan.
Normativa	Normativa relativa al documento o recurso de información. Es un enlace a un documento legal.	dct : conformsTo	–	✓	Recurso. URI que identifica al documento legal relacionado. Se pueden incluir tantas propiedades como documentos normativos se conozcan.
Distribución(es)	Referencia a los recursos que identifican los volcados del documento o recurso de información en sus posibles formatos.	dcat:distribution	✓	✓	dcat:Distribution. URI que identifica al recurso que describe una distribución del documento o recurso de información. Puede tener tantas propiedades como distribuciones se conozcan.

Distribución de documento o recurso de información (dominio dcat: Distribution)					
Metadato	**Descripción**	**propiedad**	**R**	**M**	**Tipo y Esquema de valores**
Identificador	URI que identifica a la distribución.	la dct:identifie	–	–	xsd:anyURI. URI que identifica la ficha descriptiva de la distribución.
Nombre	Breve título o nombre dado a la distribución.	dct:title	–	✓	Literal. Cadena alfanumérica (se recomienda en varios idiomas).
URL de acceso	URL que permite el acceso al volcado o consulta de los documentos o recursos de información.	dcat : accessURL	✓	–	Literal. URL con la dirección del documento, o servicio que permite la obtención de los datos.
Formato	Formato en que se encuentra representado el documento o recurso de información.	dcat:mediaType	✓	–	dct:MediaTypeOrExtent. Recurso que indica el tipo MIME del formato de los datos. Únicamente se especificará un formato por distribución.
Tamaño	Tamaño aproximado del documento o recurso de información.	dcat:byteSize	–	–	Literal. El tamaño será descrito en bytes.
Información adicional sobre formato	Enlace(s) relacionado(s) con el formato, el donde se indica el formato, el esquema utilizado para su representación u otra información técnica sobre cómo acceder a los documentos o recursos de información.	dct:relation	–	✓	Recurso. URI con una referencia a un recurso asociado con el formato. Se pueden incluir tantas propiedades como referencias a documentos adicionales se conozcan.

ANEXO IV

Metadatos de documentos y recursos de información del catálogo

Taxonomía de sectores primarios donde se especifican los temas relacionados a cada uno de ellos. Esta clasificación ha sido elaborada con base en el documento «Propuesta de Taxonomía Común para los procedimientos y servicios electrónicos, el marco de la Ley 11/2007», y comparando su propuesta de materias con las temáticas empleadas en otros portales de referencia como 060, EUGO, INE, EUROSTAT, WORLD BANK, OECD.

Esta clasificación servirá de base común para componer el esquema de URI expresado en el anexo II y para la categorización de los catálogos de recursos de información pública y sus registros, según los metadatos especificados en el anexo III.

Sector	Identificador
Ciencia y tecnología: Incluye: Innovación, Investigación, I+D+i, Telecomunicaciones, Internet y Sociedad de la Información.	ciencia-tecnologia
Comercio: Incluye: Consumo.	comercio
Cultura y ocio: Incluye: Tiempo libre.	cultura-ocio
Demografía: Incluye: Inmigración y Emigración, Familia, Mujeres, Infancia, Mayores, Padrón.	demografia
Deporte: Incluye: Instalaciones deportivas, Federaciones, Competiciones.	deporte
Economía: Incluye: Deuda, Moneda y Banca y finanzas.	economia
Educación: Incluye: Formación.	educacion
Empleo: Incluye: Trabajo, Mercado laboral.	empleo
Energía: Incluye: Fuentes renovables	energia
Hacienda: Incluye: Impuestos.	hacienda
Industria: Incluye: Minería.	industria
Legislación y justicia: Incluye: Registros.	legislacion-justicia
Medio ambiente: Incluye: Meteorología, Geografía, Conservación fauna y flora.	medio-ambiente
Medio Rural: Incluye: Agricultura, Ganadería, Pesca y Silvicultura.	medio-rural-pesca
Salud: Incluye: Sanidad.	salud
Sector público: Incluye: Presupuestos, Organigrama institucional, Legislación interna, Función pública.	sector-publico
Seguridad: Incluye: Protección civil, Defensa.	seguridad
Sociedad y bienestar: Incluye: Participación ciudadana, Marginación, Envejecimiento Activo, Autonomía personal y Dependencia, Invalidez, Jubilación, Seguros y Pensiones, Prestaciones y Subvenciones.	sociedad-bienestar
Transporte: Incluye: Comunicaciones y Tráfico.	transporte
Turismo: Incluye: Alojamientos, Hostelería, Gastronomía.	turismo
Urbanismo e infraestructuras: Incluye: Saneamiento público, Construcción (infraestructuras, equipamientos públicos).	urbanismo-infraestructuras
Vivienda: Incluye: Mercado inmobiliario, Construcción (viviendas).	vivienda

En la tabla siguiente se identifican los sectores primarios detallados anteriormente y se especifican los URI que se usarán como referencia unívoca de cada concepto. Dichos identificadores son los valores que tomarán los metadatos que categorizan por temática a los

recursos de información y que se definen en el anexo III. Esta taxonomía está definida como un esquema de conceptos identificado mediante el URI:

http://datos.gob.es/kos/sector-publico/sector

El URI de cada uno de los conceptos se compondrá concatenando la palabra que lo identifica, expresado en la tabla anterior, a la base del URI del esquema de conceptos.

Sector	URI
Ciencia y tecnología	http://datos.gob.es/kos/sector-publico/sector/ciencia-tecnologia
Comercio	http://datos.gob.es/kos/sector-publico/sector/comercio
Cultura y ocio	http://datos.gob.es/kos/sector-publico/sector/cultura-ocio
Demografía	http://datos.gob.es/kos/sector-publico/sector/demografia
Deporte	http://datos.gob.es/kos/sector-publico/sector/deporte
Economía	http://datos.gob.es/kos/sector-publico/sector/economia
Educación	http://datos.gob.es/kos/sector-publico/sector/educacion
Empleo	http://datos.gob.es/kos/sector-publico/sector/empleo
Energía	http://datos.gob.es/kos/sector-publico/sector/energia
Hacienda	http://datos.gob.es/kos/sector-publico/sector/hacienda
Industria	http://datos.gob.es/kos/sector-publico/sector/industria
Legislación y justicia	http://datos.gob.es/kos/sector-publico/sector/legislacion-justicia
Medio ambiente	http://datos.gob.es/kos/sector-publico/sector/medio-ambiente
Medio Rural	http://datos.gob.es/kos/sector-publico/sector/medio-rural-pesca
Salud	http://datos.gob.es/kos/sector-publico/sector/salud
Sector público	http://datos.gob.es/kos/sector-publico/sector/sector-publico
Seguridad	http://datos.gob.es/kos/sector-publico/sector/seguridad
Sociedad y bienestar	http://datos.gob.es/kos/sector-publico/sector/sociedad-bienestar
Transporte	http://datos.gob.es/kos/sector-publico/sector/transporte
Turismo	http://datos.gob.es/kos/sector-publico/sector/turismo
Urbanismo e infraestructuras.	http://datos.gob.es/kos/sector-publico/sector/urbanismo-infraestructuras
Vivienda	http://datos.gob.es/kos/sector-publico/sector/vivienda

ANEXO V

Metadatos de documentos y recursos de información del catálogo

Identificadores correspondientes a los recursos geográficos del territorio español –País, Autonomías y Provincias– que se utilizarán como referencia de estos elementos de forma unívoca en el proceso de descripción de los metadatos de cobertura geográfica correspondientes a los catálogos de recursos de información, según lo especificado en el anexo III; los identificadores expresados en la segunda columna de las tablas son los valores que puede tomar el metadato.

País	URI
España	http://datos.gob.es/recurso/sector-publico/territorio/Pais/España

Comunidad/Ciudad Autónoma	URI
Andalucía	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Andalucia
Aragón	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Aragon
Principado de Asturias	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Principado-Asturias
Illes Balears	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Illes-Balears
Canarias	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Canarias
Cantabria	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Cantabria
Castilla y León	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Castilla-Leon
Castilla-La Mancha	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Castilla-La-Mancha
Cataluña	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Cataluna
Comunitat Valenciana	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Comunitat-Valenciana
Extremadura	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Extremadura
Galicia	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Galicia
Comunidad de Madrid	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Comunidad-Madrid
Región de Murcia	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Region-Murcia
C. Foral de Navarra	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Comunidad-Foral-Navarra
País Vasco	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Pais-Vasco
La Rioja	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/La-Rioja
Ceuta	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Ceuta
Melilla	http://datos.gob.es/recurso/sector-publico/territorio/Autonomia/Melilla

Comunidad/Ciudad Autónoma	Provincia	URI Identificador
Andalucía	Almería	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Almeria
	Cádiz	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cadiz
	Córdoba	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cordoba
	Granada	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Granada
	Huelva	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Huelva
	Jaén	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Jaen
	Málaga	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Malaga
	Sevilla	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Sevilla
Aragón	Huesca	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Huesca
	Teruel	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Teruel
	Zaragoza	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Zaragoza
Principado de Asturias	Asturias	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Asturias
Illes Balears	Illes Balears	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Illes-Balears
Canarias	Las Palmas	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Las-Palmas
	Santa Cruz de Tenerife	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Santa-Cruz-Tenerife
Cantabria	Cantabria	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cantabria
Castilla y León	Ávila	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Avila
	Burgos	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Burgos
	León	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Leon
	Palencia	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Palencia
	Salamanca	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Salamanca
	Segovia	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Segovia
	Soria	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Soria
	Valladolid	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Valladolid
	Zamora	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Zamora
Castilla-La Mancha	Albacete	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Albacete
	Ciudad Real	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Ciudad-Real
	Cuenca	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Cuenca
	Guadalajara	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Guadalajara
	Toledo	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Toledo
Cataluña	Barcelona	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Barcelona
	Girona	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Girona
	Lleida	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Lleida
	Tarragona	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Tarragona
Comunitat Valenciana	Alicante/Alacant	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Alicante
	Castellón/Castelló	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Castellon
	Valencia/València	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Valencia
Extremadura	Badajoz	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Badajoz
	Cáceres	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Caceres
Galicia	A Coruña	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/A-Coruna
	Lugo	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Lugo
	Ourense	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Ourense
	Pontevedra	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Pontevedra
Comunidad de Madrid	Madrid	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Madrid
Región de Murcia	Murcia	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Murcia
C. Foral de Navarra	Navarra	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Navarra
País Vasco	Álava	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Alava
	Guipúzcoa	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Guipuzcoa
	Vizcaya	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Vizcaya
La Rioja	La Rioja	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/La-Rioja
Ceuta	Ceuta	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Ceuta
Melilla	Melilla	http://datos.gob.es/recurso/sector-publico/territorio/Provincia/Melilla

ANEXO VI

Modelo de plantilla RDF de definición de catálogos y registros

Modelo de plantilla para la descripción en RDF de un catálogo de datos, registros, conjuntos de datos y distribuciones asociadas. La plantilla de documento se especifica en Notación 3 (N3) y también en RDF/XML. En ambas plantillas se incluyen partes variables, así como comentarios sobre los posibles valores a utilizar. En caso de que exista alguna propiedad que no tenga aplicación o no se conozca el valor, se preferirá no definir las propiedades a dejar elementos sin valor.

Formato RDF/XML

```
<?xml version="1.0"?>
<rdf:RDF
  xmlns:time="http://www.w3.org/2006/time#"
  xmlns:dct="http://purl.org/dc/terms/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:dcat="http://www.w3.org/ns/dcat#"
  xmlns:foaf="http://xmlns.com/foaf/0.1/"
```

```
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#"
  xmlns:tema="http://datos.gob.es/kos/sector-publico/sector/"
  xmlns:auto="http://datos.gob.es/recurso/sector-publico/
territorio/Autonomia/"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">

  <dcat:Catalog rdf:about="@@URI-catalogo@@">
    <!--
      Identificador que se corresponde con el URI que
identifica a el própio catálogo
      p.e., http://datos.gob.es/catalogo/catalogoNacional
    -->
    <dct:identifier>@@URI-catalogo@@</dct:identifier>
    <!--
      El título y la descripción se puede repetir varias
veces para ofrecer representaciones en idiomas distintos
    -->
    <dct:title xml:lang="es">@@título-es@@</dct:title>
    <dct:description xml:lang="es">@@descripción@@</
dct:description>
    <!--
      Organismo que publica el catálogo, se usará un URI que
lo describe:
      p.e., http://datos.gob.es/recurso/sector-publico/org/
Organismo/E00003901
    -->
    <dct:publisher rdf:resource="@@URI-organismo@@" />
    <!--
      Tamaño del catálogo (número de datasets) expresado
mediante un entero y
      texto(s) (soporta varios idiomas).
    -->
    <dct:extent>
      <dct:SizeOrDuration>
        <rdf:value
          rdf:datatype="http://www.w3.org/2001/
XMLSchema#nonNegativeInteger">@@número-entero@@</rdf:value>
        <rdfs:label xml:lang="es">@@número-texto@@</
rdfs:label>
      </dct:SizeOrDuration>
    </dct:extent>
    <!-- Las fechas tienen el formato YYYY-MM-DDTHH:MM:SS+TZ
-->
    <dct:issued rdf:datatype="http://www.w3.org/2001/
XMLSchema#dateTime">@@fecha-creación@@</dct:issued>
    <dct:modified rdf:datatype="http://www.w3.org/2001/
XMLSchema#dateTime">@@actualización@@</dct:modified>
    <!-- Idioma del catálogo (repetir la propiedad tantas
veces como idiomas) es|ga|en|ca|...-->
    <dc:language>@@código-idioma@@</dc:language>
    <!--
      La cobertura espacial del catálogo.
      Repetir la propiedad si es necesario haciendo
referencia a un recurso del estilo:
        - http://datos.gob.es/recurso/sector-publico/
territorio/pais/Espana
        - http://datos.gob.es/recurso/sector-publico/
territorio/autonomia/Extremadura
        - http://datos.gob.es/recurso/sector-publico/
territorio/provincia/Caceres
    -->
    <dct:spatial rdf:resource="@@URI-localización@@" />
    <!--
      Taxonomía de conceptos de temáticas:
        - http://datos.gob.es/kos/sector-publico/sector/
    -->
    <dcat:themeTaxonomy rdf:resource="http://datos.gob.es/kos/
sector-publico/sector/" />
```

```
    <!-- Página principal del própio catálogo, donde se
representa visualmente -->
    <foaf:homepage rdf:resource="@@URI-homepage-catálogo@@" />
    <!-- Enlace a recurso con los términos de uso generales
(recomendable con metadatos autocontenidos) -->
    <dct:license rdf:resource="@@URI-terminos-uso@@" />
    <!--
      Especificación de cada uno de los registros contenidos
en el catálogo.
      Repetir propiedad por cada documento o recurso de
información.
    -->
    <dcat:dataset>
      <dcat:Dataset rdf:about="@@URI-dataset@@">
        <!-- Identificador que se corresponde con el URI que
identifica a el propio dataset -->
        <dct:identifier>@@URI-dataset@@</dct:identifier>
        <!-- El título y la descripción del dataset -->
        <dct:title xml:lang="es">@@título-es@@</dct:title>
        <dct:description xml:lang="es">@@descripción@@</
dct:description>
        <!--
          Temática(s) primaria(s) del catálogo. Repetir la
propiedad si hay más de una.
          Usar el esquema de conceptos normalizado:
            - http://datos.gob.es/kos/sector-publico/sector/
ciencia-tecnologia
              http://datos.gob.es/kos/sector-publico/sector/
cultura-ocio
              http://datos.gob.es/kos/sector-publico/sector/
demografia
              http://datos.gob.es/kos/sector-publico/sector/
deporte
              http://datos.gob.es/kos/sector-publico/sector/
economia
              http://datos.gob.es/kos/sector-publico/sector/
educacion
              http://datos.gob.es/kos/sector-
publico/sector/empleo
              http://datos.gob.es/kos/sector-publico/sector/
energia
              http://datos.gob.es/kos/sector-publico/sector/
hacienda
              http://datos.gob.es/kos/sector-publico/sector/
industria
              http://datos.gob.es/kos/sector-publico/sector/
legislacion-justicia
              http://datos.gob.es/kos/sector-
publico/sector/medio-ambiente
              http://datos.gob.es/kos/sector-
publico/sector/medio-rural
              http://datos.gob.es/kos/sector-
publico/sector/salud
              http://datos.gob.es/kos/sector-publico/sector/
sector-publico
              http://datos.gob.es/kos/sector-publico/sector/
seguridad
              http://datos.gob.es/kos/sector-publico/sector/
sociedad-bienestar
              http://datos.gob.es/kos/sector-publico/sector/
transporte
              http://datos.gob.es/kos/sector-publico/sector/
turismo
              http://datos.gob.es/kos/sector-publico/sector/
urbanismo-infraestructuras
              http://datos.gob.es/kos/sector-publico/sector/
vivienda
        -->
        <dcat:theme rdf:resource="@@URI-sector-temático@@" />
```

```
        <!-- Palabra(s) clave, que indica(n) conceptos
temáticos alternativos al tema primario -->
        <dcat:keyword>@@palabra-clave@@</dcat:keyword>
        <!-- Las fechas pueden ser de tipo
            - http://www.w3.org/2001/XMLSchema#date (YYYY-MM-
DD)
            - http://www.w3.org/2001/XMLSchema#dateTime (YYYY-
MM-DDTHH:MM:SS+TZ)
        -->
        <dct:issued rdf:datatype="http://www.w3.org/2001/
XMLSchema#date">@@creación@@</dct:issued>
        <dct:modified rdf:datatype="http://www.w3.org/2001/
XMLSchema#date">@@actualiz.@@</dct:modified>
        <!--
          Periodo de actualización estimada de los datos del
dataset.
          -->
          <dct:accrualPeriodicity>
          <dct:Frequency>
            <rdfs:label>Cada @@intervalo-tiempo@@</rdfs:label>
            <rdf:value>
              <time:DurationDescription>
               <rdfs:label>@@intervalo-tiempo@@</rdfs:label>
               <!-- puede ser time:days o otra magnitud
(weeks, months, etc.) -->
               <time:days rdf:datatype="http://
www.w3.org/2001/XMLSchema#decimal">@@n@@</time:days>
              </time:DurationDescription>
            </rdf:value>
          </dct:Frequency>
        </dct:accrualPeriodicity>
        <!-- Idioma(s) en los que están especificados los
datos (@@es|en|ca|ga...) -->
        <dc:language>@@idioma@@</dc:language>
        <!-- Organismo que expone los datos. Se usará un URI
que lo identifique. -->
        <dct:publisher rdf:resource="@@URI-organismo@@" />
        <!-- URI donde se describe las condiciones de uso
aplicables a los datos -->
        <dct:license rdf:resource="@@URI-licencia@@" />
        <!--
          La cobertura espacial de los datos
          Repetir la propiedad si es necesario, haciendo
referencia a un recurso del estilo:
            - http://datos.gob.es/recurso/sector-publico/
territorio/Pais/Espana
            - http://datos.gob.es/recurso/sector-publico/
territorio/Autonomia/Extremadura
            - http://datos.gob.es/recurso/sector-publico/
territorio/Provincia/Caceres
        -->
        <dct:spatial rdf:resource="@@URI-localización@@" />
        <!--
          La cobertura temporal de los datos (En el caso que
sea necesario)
          Se define el inicio y el fin mediante xsd:dateTime
(YYYY-MM-DDTHH:MM:SS+TZ)
        -->
        <dct:temporal>
          <time:Interval>
            <rdf:type rdf:resource="http://purl.org/dc/terms/
PeriodOfTime" />
            <time:hasBeginning>
              <time:Instant>
                <time:inXSDDateTime rdf:datatype="http://
www.w3.org/2001/XMLSchema#dateTime">
                    @@fecha-hora-inicio@@
                </time:inXSDDateTime>
              </time:Instant>
```

```
            </time:hasBeginning>
            <time:hasEnd>
              <time:Instant>
                 <time:inXSDDateTime rdf:datatype="http://
www.w3.org/2001/XMLSchema#dateTime">
                   @@fecha-hora-fin@@
                 </time:inXSDDateTime>
              </time:Instant>
            </time:hasEnd>
          </time:Interval>
        </dct:temporal>
        <!-- Enlaces a recursos relacionados -->
        <dct:references rdf:resource="@@URI-recurso-
relacionado@@" />
        <!--
          Las distintas distribuciones (1..n)
        -->
        <dcat:distribution>
          <dcat:Distribution>
            <!-- Identificador que se corresponde con el URI
que identifica a la propia distribución -->
            <dct:identifier>@@URI-distribución@@</
dct:identifier>
            <dct:title xml:lang="es">@@nombre-distribucion-
es@@</dct:title>
            <!-- URL de acceso a los datos -->
            <dcat:accessURL
              rdf:datatype="http://www.w3.org/2001/
XMLSchema#anyURI">@@URL-acceso@@</dcat:accessURL>
            <!-- Formato MIME de los datos de la
distribución. -->
            <dct:format>
              <dct:IMT>
                <rdf:value>${valor_MIME_Type (p.e.,
text/csv)}</rdf:value>
                <rdfs:label>${texto_legible_ (p.e., CSV)}</
rdfs:label>
              </dct:IMT>
            </dct:format>
            <!--
              Tamaño de la distribución del documento o
recurso de información.
              Se representa en bytes (número decimal) y con
una etiqueta textual legible (p.e., 30KB)
            -->
            <dcat:byteSize rdf:datatype="http://
www.w3.org/2001/XMLSchema#decimal">
                  @@num-bytes@@
            </dcat:byteSize>
            <!--
              Si se conoce algún documento con información
adicional sobre los datos y el
              acceso a los mismos, se puede hacer referencia
mediante un texto y la URL al documento
            -->
            <dct:relation>
              <rdf:Description>
                <rdfs:label xml:lang="es">@@texto-enlace@@</
rdfs:label>
                <foaf:page rdf:resource="@@URL-documento@@" />
              </rdf:Description>
            </dct:relation>
          </dcat:Distribution>
        </dcat:distribution>
      </dcat:Dataset>
    </dcat:dataset>
  </dcat:Catalog>
</rdf:RDF>
```

Notación 3 (N3)

```
@prefix dct: <http://purl.org/dc/terms/>.
@prefix dc: <http://purl.org/dc/elements/1.1/>.
@prefix dcat: <http://www.w3.org/ns/dcat#>.
@prefix foaf: <http://xmlns.com/foaf/0.1/>.
@prefix xsd: <http://www.w3.org/2001/XMLSchema#>.
@prefix tema: <http://datos.gob.es/kos/sector-
publico/sector/>.
@prefix time: <http://www.w3.org/2006/time#>.
@prefix xml: <http://www.w3.org/XML/1998/namespace>.
@prefix rdfs: <http://www.w3.org/2000/01/rdf-schema#>.
@prefix rdf: <http://www.w3.org/1999/02/22-rdf-syntax-ns#>.
@prefix auto: <http://datos.gob.es/recurso/sector-publico/
territorio/Autonomia/>.


#El catálogo
$$URI-catalogo$$ a dcat:Catalog;
   dct:title "$$título-es$$"@es;
   dct:description "$$descripción$$"@es;
   dct:identifier "$$URI-catalogo";
   # Número de conjuntos de datos
   dct:extent
   [
      a dct:SizeOrDuration;
      rdf:value "$$número-entero$$"^^xsd:nonNegativeInteger;
      rdfs:label "$$número-texto$$"@es.
   ];
   # Fechas de creación y actualización
   dct:issued "$$fecha-creación$$"^^xsd:dateTime;
   dct:modified "$$actualización$$"^^xsd:dateTime;
   dc:language "$$código-idioma$$";
   dct:publisher <$$URI-organismo$$>;
   dct:license <$$URI-términos-uso$$>;
   dct:spatial <$$URI-localización$$>;
   dcat:themeTaxonomy <http://datos.gob.es/kos/sector-
publico/sector/>;
   foaf:homepage <$$URI-homepage-catálogo$$>;

   # Conjuntos de datos que pertenecen al catálogo
(múltiples)
   dcat:dataset <$$URI-dataset$$>.


# Los conjuntos de datos asociados al catálogo
<$$URI-dataset$$> a dcat:Dataset;
   dct:title "$$título-es$$"@es;
   dct:description "$$descripción$$"@es;
   dcat:theme <$$URI-sector-temático$$>;
   dcat:keyword "$$palabra-clave$$","$$palabra-clave2$$","$
$palabra-claveN$$";
   # Frecuencia de actualización aproximada
   dct:accrualPeriodicity
   [
      a dct:Frequency;
      rdf:value
      [
         a time:DurationDescription;
         rdfs:label "$$intervalo-tiempo$$";
         time:days $$n$$.
      ];
      rdfs:label "Cada $$intervalo-tiempo$$".
   ];
   dct:publisher <$$URI-organismo$$>;
   dct:identifier "$$URI-dataset$$";
   dct:issued "$$creació$$"^^xsd:date;
   dct:modified "$$actualización$$"^^xsd:date;
```

```
   dc:language "$$idioma$$";
   dct:license <$$URI-licencia$$>;
   dct:spatial <$$URI-localización$$>;
   dct:references <$$URI-dataset$$>;
   dct:temporal
   [
      a dct:PeriodOfTime, time:Interval;
      time:hasBeginning
      [
         a time:Instant;
         time:inXSDDateTime "$$fecha-hora-inicio$
$"^^xsd:dateTime.
      ];
      time:hasEnd
      [
         a time:Instant;
         time:inXSDDateTime "$$fecha-hora-fin$
$"^^xsd:dateTime.
      ].
   ];
   # Cada una de las distribuciones del documento o recurso
de información
   dcat:distribution
   [
      a dcat:Distribution;
      dct:identifier "$$URI-distribución$$";
      dct:title "$$nombre-distribucion-es$$"@es;
      dct:format
      [
         a dct:IMT;
         rdf:value "${valor_MIME_Type (p.e., text/csv)}";
         rdfs:label "${texto_legible_ (p.e., CSV)}".
      ];
      dct:relation
      [
         rdfs:label "$$texto-enlace$$"@es;
         foaf:page <$$URL-documento$$>.
      ];
      dcat:accessURL "$$URL-acceso$$"^^xsd:anyURI;
      dcat:byteSize "$$num-bytes-texto$$".   ].
```

§ 39

Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 265, de 2 de noviembre de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-10108

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

El Real Decreto 3/2010, de 8 de enero, prevé en su artículo 29 apartado 2 que el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Dichas instrucciones técnicas de seguridad son esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema.

Así, estas instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; notificación de incidentes de Seguridad; auditoría de la Seguridad; conformidad con el Esquema Nacional de Seguridad; adquisición de Productos de Seguridad; criptología de empleo en el Esquema Nacional de Seguridad; interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la Instrucción Técnica de Seguridad de Informe Nacional del Estado de la Seguridad, establece las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas

comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas, al objeto de poder dar adecuada respuesta al mandato del artículo 35 del Real Decreto 3/2010, de 8 de enero.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29 apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional. En virtud de lo anterior, esta Secretaría de Estado resuelve:

Primero.

Aprobar la Instrucción Técnica de Seguridad «Informe del Estado de la Seguridad», cuyo texto se incluye a continuación.

Segundo.

Ordenar su publicación en el «Boletín Oficial del Estado».

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE INFORME DEL ESTADO DE LA SEGURIDAD

I. Objeto: La Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad tiene por objeto establecer las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas.

II. Ámbito de aplicación: La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en lo dispuesto en el artículo 3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

III. Recopilación y comunicación de datos:

III.1 Las entidades públicas comprendidas en el ámbito de aplicación de la presente Instrucción Técnica de Seguridad recopilarán los datos de las diferentes variables de seguridad conforme a lo dispuesto en la medida «sistema de métricas [op.mon.2]» del Anexo II del Real Decreto 3/2010, de 8 de enero.

III.2 Las entidades públicas a las que se refiere el punto anterior comunicarán, al menos con carácter anual, el estado de las principales variables de seguridad de aquellos sistemas de información que se encuentren bajo su responsabilidad.

III.3 Para la comunicación a la que se refiere el punto anterior, el Responsable de Seguridad de los sistemas de información afectados de la entidad pública, o en quien este delegue, utilizará la herramienta relativa al Informe Nacional del Estado de la Seguridad (INES), al que tendrá acceso, previa identificación, en el siguiente enlace: https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ines.html

III.4 El Centro Criptológico Nacional, en cumplimiento del artículo 29 apartado 1 del Real Decreto 3/2010, de 8 de enero mantendrá un Manual de Usuario de la herramienta INES, permanentemente actualizado a través de la guía de seguridad CCN-STIC 844.

IV. Tratamiento de datos:

IV.1 Los datos que la herramienta INES requerirá de la entidad pública del ámbito de aplicación de la presente Instrucción Técnica de Seguridad son los que se señalan en la guía de seguridad CCN-STIC 824 Informe del Estado de Seguridad, que el Centro Criptológico Nacional mantendrá permanentemente actualizada y, en general, estarán referidos a identificación de la entidad, datos generales, organización de la seguridad, procesos críticos, concienciación y formación, gestión de incidentes, recursos y presupuestos, auditoría, indicadores críticos de riesgo y medidas de seguridad, según lo descrito en la guía de seguridad CCN-STIC-815 sobre Métricas e Indicadores para el Esquema Nacional de Seguridad.

§ 40

Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 265, de 2 de noviembre de 2016
Última modificación: sin modificaciones
Referencia: BOE-A-2016-10109

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, recoge el Esquema Nacional de Seguridad en su artículo 156 apartado 2 en similares términos.

El Real Decreto 3/2010, de 8 de enero, prevé en su artículo 29 apartado 2 que el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante resolución de la Secretaría de Estado de Administraciones Públicas. Dichas instrucciones técnicas de seguridad son esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el Esquema.

Así, estas instrucciones técnicas de seguridad, enumeradas en la disposición adicional cuarta del citado Real Decreto, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; notificación de incidentes de Seguridad; auditoría de la Seguridad; conformidad con el Esquema Nacional de Seguridad; adquisición de Productos de Seguridad; criptología de empleo en el Esquema Nacional de Seguridad; interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad establece los criterios y procedimientos para la determinación de la

conformidad con el Esquema Nacional de Seguridad y para la publicidad de dicha conformidad, al objeto de poder dar adecuada respuesta al mandato del Capítulo VIII, Normas de conformidad, del Real Decreto 3/2010, de 8 de enero; así, determina los mecanismos de obtención y ulterior publicidad de las declaraciones de conformidad y los distintivos de seguridad de los que sean acreedores y que se hubieren obtenido respecto al cumplimiento del Esquema Nacional de Seguridad.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29 apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional. En virtud de lo anterior, esta Secretaría de Estado resuelve:

Primero.

Aprobar la Instrucción Técnica de Seguridad «Conformidad con el Esquema Nacional de Seguridad», cuyo texto se incluye a continuación.

Segundo.

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

I. Objeto

La Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad tiene por objeto establecer los procedimientos para dar publicidad a la conformidad con el Esquema Nacional de Seguridad, así como los requisitos exigibles a las entidades certificadoras.

II. Ámbito de aplicación

La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en lo dispuesto en el artículo 3 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

III. Procedimientos de determinación de la conformidad

III.1 En función de la categoría de los sistemas de información del ámbito de aplicación del Esquema Nacional de Seguridad, de acuerdo con el Anexo I del Real Decreto 3/2010, de 8 de enero, se define el procedimiento de determinación de la conformidad. Así los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, mientras que los sistemas de categoría MEDIA O ALTA precisarán de una auditoría formal para su certificación de la conformidad.

III.2 La declaración de la conformidad con el Esquema Nacional de Seguridad de los sistemas de información con categoría BÁSICA se realizará mediante una autoevaluación que, con carácter ordinario, verifique el cumplimiento de los requerimientos contemplados en el Esquema, al menos cada dos años. Dicha autoevaluación atenderá a lo dispuesto sobre auditoría en el artículo 34 y en el anexo III del Real Decreto 3/2010, de 8 de enero. Dicha autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.

III.3 La certificación de la conformidad con el Esquema Nacional de Seguridad de los sistemas de información con categorías MEDIA o ALTA se realizará mediante un procedimiento de auditoría formal que, con carácter ordinario, verifique el cumplimiento de

los requerimientos contemplados en el Esquema, al menos cada dos años. Dicha auditoría se realizará según lo dispuesto en el artículo 34 y en el anexo III del Real Decreto 3/2010, de 8 de enero.

III.4 Siendo obligatoria la auditoría formal para los sistemas de categoría MEDIA Y ALTA nada impide que un sistema de categoría BÁSICA se someta igualmente a una auditoria formal de certificación de la conformidad, siendo esta posibilidad siempre la deseable.

III.5 En las comunidades autónomas con lengua cooficial se podrán expedir las declaraciones, certificaciones y sus respectivos distintivos de conformidad en castellano o bien en texto bilingüe. En este caso, se expedirán en un solo documento redactado en castellano y en la correspondiente lengua cooficial, en tipos de letra de igual rango con las especificaciones y diligencias que sobre su texto se establecen en los anexos correspondientes.

IV. Declaración de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA y su publicidad

IV.1 La Declaración de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría BÁSICA o inferior será expedida por la propia entidad bajo cuya responsabilidad se encuentren dichos sistemas, y se completará mediante un Distintivo de Declaración de Conformidad cuyo uso estará condicionado a la antedicha Declaración de Conformidad.

IV.2 Dicha Declaración de Conformidad así como su distintivo se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos I y II respectivamente de la presente Instrucción Técnica de Seguridad.

IV.3 Para publicar la Declaración de Conformidad con el Esquema Nacional de Seguridad en el caso de sistemas de información de categoría BÁSICA o inferior bastará con la exhibición en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Declaración de Conformidad que incluirá un enlace al documento de Declaración de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

V. Certificación de Conformidad con el Esquema Nacional de Seguridad de sistemas de categoría MEDIA o ALTA y su publicidad

V.1 La Certificación de Conformidad con el Esquema Nacional de Seguridad, de sistemas de categorías MEDIA o ALTA, será expedida por una entidad certificadora y se completará mediante un Distintivo de Certificación de Conformidad cuyo uso estará condicionado a la antedicha Certificación de Conformidad.

V.2 Dicha Certificación de Conformidad así como su distintivo se expresarán en documentos electrónicos, en formato no editable y poseerán el aspecto que se muestra en los Anexos III y IV respectivamente de la presente Instrucción Técnica de Seguridad.

V.3 Para publicar la Certificación de Conformidad con el Esquema Nacional de Seguridad en el caso de sistemas de información de categoría MEDIA O ALTA bastará con la exhibición en la sede electrónica de la entidad pública titular o usuaria del sistema de información en cuestión, del Distintivo de Certificación de Conformidad que incluirá un enlace al documento de Certificación de Conformidad correspondiente, que también permanecerá accesible a través de dicha sede electrónica.

VI. Requisitos de las entidades certificadoras

VI.1 Las entidades certificadoras a las que se refiere esta Instrucción Técnica deberán estar acreditadas por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas del ámbito de aplicación del Esquema Nacional de Seguridad conforme a la norma UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios.

VI.2 Si la entidad certificadora de que se trate no dispusiere de la acreditación señalada, previamente a iniciar sus actividades, deberá remitir al Centro Criptológico Nacional, la aceptación por parte de la Entidad Nacional de Acreditación de haber solicitado la

acreditación antedicha, pudiendo iniciar sus actividades de certificación de forma transitoria, disponiendo de 12 meses para obtener dicha acreditación, transcurridos los cuales sin haberla obtenido deberán cesar en sus actividades de certificación. El Centro Criptológico Nacional podrá requerir a la entidad certificadora solicitante cuanta información adicional considere necesaria que le permita verificar su adecuación y suficiencia.

VI.3 Transcurrido un año desde la entrada en vigor de la presente Instrucción Técnica de Seguridad, ya no será posible iniciar ningún proceso de certificación de la forma transitoria señalada en el punto anterior, exigiéndose a todas las entidades de certificación la acreditación recogida en el punto VI.1.

VI.4 Estarán exentas del cumplimiento de los requisitos señalados en los puntos anteriores del presente epígrafe aquellas entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias incluyan el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

VI.5 El Centro Criptológico Nacional mantendrá en su sede electrónica una relación actualizada de las Entidades de Certificación, acreditadas o en vías de acreditación, para expedir Certificaciones de Conformidad con el Esquema Nacional de Seguridad.

VII. Soluciones y servicios prestados por el sector privado

VII.1 Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas.

VIII.2 Es responsabilidad de las entidades públicas contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, según lo señalado en la presente Instrucción Técnica de Seguridad.

VII.3 Cuando la provisión de las soluciones o la prestación de los servicios sujetos al cumplimiento del Esquema Nacional de Seguridad sean realizados por operadores del sector privado, estos utilizarán los mismos modelos documentales utilizados para las Declaraciones, las Certificaciones o los Distintivos de Conformidad recogidos en la presente Instrucción Técnica de Seguridad, sustituyendo las referencias a las entidades públicas por las correspondientes a las entidades privadas. Análogamente, los Distintivos de Conformidad, cuando se exhiban por parte de dichos operadores privados, deberán enlazar con las correspondientes Declaraciones o Certificaciones de Conformidad, que permanecerán siempre accesibles en la página electrónica del operador de que se trate.

VII.4 Además del Centro Criptológico Nacional y la Entidad Nacional de Acreditación, las entidades públicas usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado que exhiban una Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad podrán solicitar en todo momento a tales operadores los Informes de Autoevaluación o Auditoría correspondientes, al objeto de verificar la adecuación e idoneidad de las antedichas manifestaciones.

ANEXO I

Contenido de la Declaración de Conformidad con el Esquema Nacional de Seguridad

Cada entidad u organismo declarante podrá disponer libremente de su propio formato de Declaración de Conformidad con el Esquema Nacional de Seguridad, que deberá mostrar, al menos, el contenido siguiente:

– Logotipo de la entidad u organismo declarante.
– Identificación de la entidad u organismo declarante.
– Distintivo de Declaración de Conformidad de acuerdo al anexo II de esta Instrucción Técnica de Seguridad.
– Texto: “Declaración de Conformidad con el Esquema Nacional de Seguridad”.
– Texto: “Los sistemas de información reseñados, todos ellos de categoría BÁSICA, y los servicios que se relacionan, han superado un proceso de autoevaluación conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de <>:”

– <>.

– Texto: “Fecha de declaración de conformidad inicial: <> de <> de <>”
– Texto: “Fecha de renovación de la declaración de conformidad: <> de <> de <>”.
– Texto: “Fecha: <>, <> de <> de <>”.
– Firma: <>.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la Declaración de Conformidad expedida.

La guía de seguridad CCN-STIC 809 sobre declaración y certificación de conformidad con el Esquema Nacional de Seguridad y distintivos de cumplimiento ofrecerá modelos ilustrativos de la citada Declaración de conformidad.

ANEXO II

Distintivo de Declaración de Conformidad con el Esquema Nacional de Seguridad

En la medida de lo posible, los Distintivos de Declaración de Conformidad con el Esquema Nacional de Seguridad que se exhiban en medios electrónicos o en papel respetarán las proporciones, formas, tipografía y colores de la imagen anterior.

Colores directos	CMYK	RGB	Hexadecimal
Pantone Orange 021C	C: 0	R: 235	FF6600
	M: 53	G: 111	
	Y: 100	B: 12	
	K: 0		

ANEXO III

Contenido de la Certificación de Conformidad con el Esquema Nacional de Seguridad

Cada Entidad Certificadora podrá disponer libremente de su propio formato de Certificación de Conformidad con el Esquema Nacional de Seguridad, que deberá mostrar, al menos, el contenido siguiente:

– Logotipo de la Entidad Certificadora.
– Identificación de la Entidad Certificadora.
– Distintivo de Certificación de Conformidad de acuerdo al anexo IV de esta Instrucción Técnica de Seguridad.
– Texto: “Certificado de Conformidad con el Esquema Nacional de Seguridad”.
– Texto: “<> certifica que los sistemas de información reseñados, todos ellos de categoría <>, y los servicios que se relacionan, de <>, han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría de <>:”

– <>.

– Texto: “Número de certificado: <>”.
– Texto: “Fecha de certificación de conformidad inicial: <> de <> de <>”.
– Texto: “Fecha de renovación de la certificación de conformidad: <> de <> de <>”.
– Texto: “Fecha: <>, <> de <> de <>”.
– Firma: Nombre y Apellidos del responsable competente de la Entidad Certificadora.

Los textos que aparecen entre paréntesis angulares se adaptarán a los aspectos concretos de la certificación expedida.

La guía de seguridad CCN-STIC 809 sobre declaración y certificación de conformidad con el Esquema Nacional de Seguridad y distintivos de cumplimiento ofrecerá modelos ilustrativos de la citada Certificación de conformidad.

ANEXO IV

Distintivo de Conformidad con el Esquema Nacional de Seguridad

En la medida de lo posible, los Distintivos de Certificación de Conformidad con el Esquema Nacional de Seguridad que se exhiban en medios electrónicos o en papel respetarán las proporciones, formas, tipografía y colores de la imagen anterior.

Colores directos	CMYK	RGB	Hexadecimal
Pantome 653C	C: 82	R: 55	336699
	M: 47	G: 99	
	Y: 11	B: 150	
	K: 0		

§ 41

Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información

Ministerio de Hacienda y Función Pública
«BOE» núm. 81, de 3 de abril de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-4573

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho Real Decreto prevé, en su artículo 29, apartado 2, que el Ministerio de Hacienda y Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante resolución de la Secretaría de Estado de Función Pública, constituyendo elementos esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así pues, tales instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto 3/2010, de 8 de enero, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; Notificación de Incidentes de Seguridad; Auditoría de la Seguridad; Conformidad con el Esquema Nacional de Seguridad; Adquisición de Productos de Seguridad; Criptología de empleo en el Esquema Nacional de Seguridad; Interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar la Comisión Sectorial de administración electrónica, según lo establecido en el citado artículo 29, en relación con lo dispuesto en la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y Disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración Electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la instrucción técnica de seguridad de Auditoría de la Seguridad de los sistemas de información establece las condiciones para la realización de la preceptiva

auditoría a la que deben someterse los sistemas de información del ámbito de aplicación del ENS, tal y como se regula en el artículo 34 y Anexo III de su norma reguladora.

Por otra parte, de acuerdo con el Real Decreto 769/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales corresponde a la Secretaría de Estado de Función Pública el impulso, la programación y la supervisión de las actuaciones en ejecución de la política de Gobierno en materia de Administración Digital y del fomento de la administración electrónica, en especial lo referente al proceso de racionalización de las tecnologías de la información y de las comunicaciones, y la adopción de soluciones digitales que permitan la prestación eficiente de los servicios públicos incluyendo los servicios públicos esenciales.

Esta Resolución se aprueba en aplicación de lo dispuesto en el Real Decreto 3/2010, de 8 de enero, en el artículo 29, apartado 2, en el capítulo V, Auditoría de la seguridad, artículo 34, así como en su Anexo III, modificado por Real Decreto 951/2015, de 23 octubre, a propuesta de la Comisión Sectorial de Administración Electrónica.

En virtud de lo anterior, esta Secretaría de Estado resuelve:

Primero.

Aprobar la Instrucción Técnica de Seguridad «Auditoría de la Seguridad de los sistemas de información», cuyo texto se incluye a continuación.

Segundo.

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los sistemas de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE AUDITORÍA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

ÍNDICE

I. Objeto: La Instrucción Técnica de Seguridad de Auditoría de la Seguridad tiene por objeto establecer las condiciones para la realización de las auditorías, ordinarias o extraordinarias, previstas en el artículo 34 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

II. Ámbito de aplicación: La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación del Real Decreto 3/2010, de 8 de enero, según dispone el artículo 3 del mismo, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015,de 1 de octubre, de Régimen Jurídico del Sector Público.

III. Propósito de la Auditoría de la Seguridad, obligatoriedad y normativa reguladora:

III.1 La Auditoría de la Seguridad es un proceso sistemático, independiente y documentado, para la obtención de evidencias y su evaluación objetiva, con el fin de determinar el grado de conformidad con el ENS del sistema de información auditado. Debe

permitir a sus responsables adoptar las medidas oportunas para subsanar las deficiencias y atender a las observaciones o recomendaciones que pudiera haber identificado el Equipo Auditor y, en su caso, posibilitar la obtención de la correspondiente Certificación de Conformidad, tal y como dispone la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, regulada por Resolución de 13 de octubre de 2016, del Secretario de Estado de Administraciones Públicas.

III.2 Para obtener la Certificación de Conformidad con el ENS, los sistemas de información de categorías MEDIA o ALTA precisarán superar una Auditoría de Seguridad, al menos cada dos años. Los sistemas de información de categoría BÁSICA solo requerirán de una autoevaluación que, de ser favorable, permitirá la exhibición de la Declaración de Conformidad, y cuyo resultado deberá estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular, así como las evidencias que sustentan la valoración anterior. Dicha autoevaluación podrá ser desarrollada por el mismo personal que administra el sistema de información o en quién éste delegue.

III.3 Siendo obligatoria la Auditoría de Seguridad para los sistemas de categorías MEDIA o ALTA, nada impide que un sistema de categoría BÁSICA se someta asimismo a un proceso de Auditoría de Seguridad para la Certificación de la Conformidad, siendo siempre esta posibilidad la deseable.

III.4 El desarrollo de la Auditoría de la Seguridad se realizará con sujeción a la normativa contenida en la presente Instrucción Técnica de Seguridad y complementariamente, cuando corresponda, atendiendo a las normas nacionales e internacionales sobre auditoría de sistemas de información, entre ellas las guías CCN-STIC 802 Guía de auditoría, CCN-STIC 804 Guía de Implantación y CCN-STIC 808 Verificación del cumplimiento de las medidas en el ENS, y aquellas otras de ética y control de calidad interna de los auditores y entidades de auditoría, certificación y acreditación.

IV. Definición del alcance y objetivo de la Auditoría de la Seguridad:

IV.1 Los criterios metodológicos de auditoría utilizados, el alcance y objetivo de la Auditoría de la Seguridad deberán estar claramente definidos y documentados, conforme a lo dispuesto en el artículo 34 y en el Anexo III del ENS, debiendo aparecer en el Informe de Auditoría que se obtenga.

IV.2 Para asegurar la independencia objetiva de la Entidad Certificadora, las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas actividades de consultoría o similares, tales como implantación o modificación de aplicaciones, relacionadas con el sistema auditado, redacción de documentos requeridos por el ENS o procedimientos de actuación, así como recomendaciones particulares sobre productos o soluciones concretas, entre otros.

V. Ejecución de la Auditoría de la Seguridad:

V.1 La entidad titular del sistema de información a auditar facilitará a la Entidad Certificadora cuanta información fuera pertinente para realizar los trabajos de auditoría, teniendo en cuenta su alcance y las eventuales limitaciones derivadas del ordenamiento jurídico.

V.2 El Equipo Auditor está obligado a requerir y obtener las evidencias pertinentes para verificar los criterios de auditoría, cuya evaluación constituirán los hallazgos en que se basarán las conclusiones recogidas en el Informe de Auditoría.

VI. El Informe de Auditoría:

VI.1 Atendiendo a la categoría del sistema auditado (BÁSICA, MEDIA o ALTA) el dictamen sobre la conformidad con el ENS se basará en el cumplimiento de los preceptos contenidos en el RD 3/2010, de 8 de enero, y de las medidas de seguridad del Anexo II del ENS que resulten de aplicación, así como de aquellos requisitos específicos que pudieran documentarse en guías CCN-STIC en función del contexto interno o externo del sistema de información, identificando, en su caso, las desviaciones que se observen, así como los registros, declaraciones de hechos o cualquier otra información pertinente y verificable en que se basen las conclusiones alcanzadas.

VI.2 Los hallazgos de no conformidad se clasificarán atendiendo a los siguientes grados:

– «No Conformidad Menor»: Se documentará una «No Conformidad Menor» ante la ausencia o el fallo en la implantación o mantenimiento de uno o más de los requisitos del ENS, incluyendo cualquier situación que pudiese, en base a una evidencia objetiva, sustentar una duda significativa sobre la conformidad del sistema de información con uno o más de tales requisitos.

– «No Conformidad Mayor»: Se documentará una «No Conformidad Mayor» cuando se detecten «No Conformidades Menores» en relación con cualquiera de los preceptos contenidos en el RD 3/2010, de 8 de enero, o en el Marco organizativo, o en alguno de los subgrupos que integran el Marco operacional o las Medidas de protección (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, Monitorización del Sistema, Protección de las Infraestructuras, Gestión del Personal, Protección de Equipos, Comunicaciones, Soportes de Información, Aplicaciones Informáticas, Información o Servicios) que, evaluadas en su conjunto, puedan implicar el incumplimiento del objetivo del Grupo o Subgrupo considerados.

Se documentará una Observación cuando se encuentren evidencias de una debilidad, una vulnerabilidad o una situación que, sin comprometer cualquier área del sistema de gestión definida en el ENS o por la organización, pueda, en la actualidad o en el futuro, derivar en un problema.

VI.3 El dictamen final de la Auditoría de la Seguridad será uno de los tres siguientes:

– «FAVORABLE»: Cuando no se evidencie ninguna «No Conformidad Mayor» o «No Conformidad Menor».

– «FAVORABLE CON NO CONFORMIDADES»: Cuando se evidencie cualquier no conformidad, mayor o menor. En este caso, la entidad titular responsable del sistema de información auditado deberá presentar, en el plazo máximo de un mes, un Plan de Acciones Correctivas sobre tales hallazgos de no conformidad a la entidad certificadora para su evaluación.

– «DESFAVORABLE»: Cuando, por el número o la transcendencia de las no conformidades detectadas, no sea posible decidir sobre su resolución a través de un Plan de Acciones Correctivas. En este caso se requerirá la realización de una auditoría extraordinaria que verifique la adopción de las medidas correctoras adecuadas.

La Guía CCN-STIC 824 Informe del Estado de Seguridad, que el Centro Criptológico Nacional mantendrá permanentemente actualizada, ofrecerá pautas de ayuda para el dictamen final de la Auditoría de la Seguridad.

VI.4 La Certificación de Conformidad con el ENS únicamente podrá expedirse si el dictamen fuera «FAVORABLE» o, si habiendo sido «FAVORABLE CON NO CONFORMIDADES», el Plan de Acciones Correctivas presentado por la entidad titular del sistema de información, trata y resuelve los hallazgos de no conformidad evidenciados, a criterio de la entidad certificadora.

VI.5 Ante un dictamen «DESFAVORABLE», la entidad titular del sistema de información auditado, en un plazo no superior a seis meses desde la fecha de emisión del Informe de Auditoría, deberá someterse a una Auditoría Extraordinaria, exclusivamente sobre los hallazgos de no conformidad evidenciados que, de resultar satisfactorio, permitirá la expedición del correspondiente Certificado de Conformidad con el ENS.

VI.6 En caso de un sistema certificado sobre el que se detecten No Conformidades Mayores, durante el período de resolución de las No Conformidades Mayores el Certificado de Conformidad quedará en suspenso. En caso de no cerrar las No Conformidades Mayores en un plazo de seis meses el Certificado de Conformidad quedaría revocado y la entidad auditada deberá eliminar el Distintivo de Conformidad de su sede hasta su próxima recertificación.

VI.7 El informe de Auditoría deberá contener la información adecuada y suficiente para facilitar y justificar la decisión de certificación, como mínimo:

– Las áreas organizativas, módulos o funciones del sistema de información cubiertas por la auditoría, incluyendo los requisitos de certificación y las ubicaciones que fueron auditadas, las pistas de auditoría seguidas y las metodologías de auditoría utilizadas.

– Los hallazgos identificados, tanto de conformidad como de no conformidad, incluyendo las Observaciones.

– Los detalles de las no conformidades identificadas se justificarán mediante evidencias objetivas y su correspondencia con los requisitos del ENS u otros documentos requeridos para la Certificación.

– Comentarios sobre la conformidad del Sistema de Gestión de Seguridad de la Información del auditado con los requisitos de certificación, con una redacción clara de las no conformidades que hubieran podido evidenciarse, una referencia a la versión de la Declaración de Aplicabilidad, que incluya el nivel en cada dimensión para cada medida de seguridad del ENS aplicable, así como cualquier comparación útil con los resultados de Auditorías de la Seguridad previas.

– La Categoría del Sistema, con detalle del nivel de seguridad en cada una de las dimensiones recogidas en el ENS.

– El grado de confianza en las revisiones de la Dirección y auditorías internas del auditado.

– La conclusión o dictamen del Equipo de Auditoría sobre si el sistema de información del auditado debe ser certificado o no, con información que soporte esa conclusión.

VI.8 Los informes de auditoría podrán ser requeridos por el CCN-CERT, en los términos previstos en el artículo 37 del ENS.

VII. Entidades Auditoras del Sector Público: La presente Instrucción Técnica de Seguridad también será de aplicación a las actividades de auditoría y a la emisión de los correspondientes informes que se realicen por entidades, órganos, organismos y unidades vinculadas o dependientes de las Administraciones Públicas cuyas competencias se correspondan con el desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

VIII. Disposición adicional. Datos personales:

VIII.1 Cuando el sistema auditado tenga por objeto o incluya el tratamiento de datos personales se tendrá en cuenta lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo.

VIII.2 A partir del 25 de mayo de 2018, cuando el sistema auditado tenga por objeto o incluya el tratamiento de datos personales, se tendrá en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. A partir de dicha fecha en todo momento se informará al Delegado de Protección de Datos en calidad de responsable de la supervisión del cumplimiento del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

§ 42

Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad

Ministerio de Hacienda y Función Pública
«BOE» núm. 95, de 19 de abril de 2018
Última modificación: sin modificaciones
Referencia: BOE-A-2018-5370

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, ENS en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dicho Real Decreto prevé, en su artículo 29, apartado 2, que el Ministerio de Hacienda y Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante resolución de la Secretaría de Estado de Función Pública, constituyendo elementos esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así pues, tales instrucciones técnicas de seguridad, enumeradas en la Disposición Adicional cuarta del citado Real Decreto 3/2010, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como: Informe del Estado de la Seguridad; Notificación de Incidentes de Seguridad; Auditoría de la Seguridad; Conformidad con el Esquema Nacional de Seguridad; Adquisición de Productos de Seguridad; Criptología de empleo en el Esquema Nacional de Seguridad; Interconexión en el Esquema Nacional de Seguridad y Requisitos de Seguridad en entornos externalizados, sin perjuicio de las propuestas que pueda acordar la Comisión Sectorial de administración electrónica, según lo establecido en el citado artículo 29, en relación con lo dispuesto en la Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas y Disposición adicional novena de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Estas instrucciones técnicas de seguridad se desarrollarán y perfeccionarán a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, las infraestructuras que los apoyan, la evolución tecnológica y los riesgos derivados de operar en el ciberespacio.

En particular, la instrucción técnica de seguridad de Notificación de Incidentes de Seguridad establece los criterios y procedimientos para la notificación por parte de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público al Centro Criptológico Nacional (CCN) de aquellos incidentes que tengan un impacto significativo en la seguridad de la información que manejan y los servicios que prestan en relación con la categoría del sistema, al objeto de poder dar adecuada respuesta al mandato del Capítulo VII, Respuesta a incidentes de seguridad, del Real Decreto 3/2010, de 8 de enero.

Por otra parte, de acuerdo con el Real Decreto 769/2017, de 28 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Función Pública y se modifica el Real Decreto 424/2016, de 11 de noviembre, por el que se establece la estructura orgánica básica de los departamentos ministeriales corresponde a la Secretaría de Estado de Función Pública el impulso, la programación y la supervisión de las actuaciones en ejecución de la política de Gobierno en materia de Administración Digital y del fomento de la administración electrónica, en especial lo referente al proceso de racionalización de las tecnologías de la información y de las comunicaciones, y la adopción de soluciones digitales que permitan la prestación eficiente de los servicios públicos incluyendo los servicios públicos esenciales. Además, dado que la resolución impone obligaciones no solo en el ámbito competencial de esta Secretaria de Estado sino también al Centro Criptológico Nacional (CCN) integrado en el CNI, organismo adscrito al Ministerio de la Presidencia y para las Administraciones Territoriales procede recabar el parecer del citado Departamento.

Esta Resolución se aprueba en aplicación de lo dispuesto en el artículo 29, apartado 2 del Real Decreto 3/2010, de 8 de enero, a propuesta de la Comisión Sectorial de Administración Electrónica y habiéndose solicitado informe al Ministerio de la Presidencia y para las Administraciones Territoriales.

En virtud de lo anterior, esta Secretaría de Estado resuelve:

Primero.

Aprobar la Instrucción Técnica de Seguridad «Notificación de incidentes de seguridad», cuyo texto se incluye a continuación.

Segundo.

Ordenar su publicación en el «Boletín Oficial del Estado».

La Instrucción Técnica de Seguridad de Notificación de incidentes de seguridad de los sistemas de información que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

INSTRUCCIÓN TÉCNICA DE SEGURIDAD DE NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD

ÍNDICE

I. Objeto

La Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad tiene por objeto, según lo dispuesto en el Capítulo VII del Real Decreto 3/2010, de 8 de enero, la notificación y gestión de incidentes de seguridad en los sistemas de información de las entidades del Sector Público del ámbito de aplicación de dicho cuerpo legal, cuando tales

incidentes tengan un impacto significativo en la seguridad de la información que manejan o los servicios que prestan, en relación con la categoría del sistema y con independencia de los requerimientos adicionales que cada organismo o entidad implemente para adaptarlos a sus entornos singulares.

II. Ámbito de aplicación

La presente Instrucción Técnica de Seguridad será de aplicación a los sistemas de información comprendidos en los ámbitos subjetivo y objetivo de aplicación del Real Decreto 3/2010, de 8 de enero, según dispone el artículo 3 del mismo, así como al resto de las entidades que forman parte de los ámbitos subjetivos de aplicación de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

III. Criterios de determinación del nivel de Impacto

Una vez detectado un incidente se utilizará la Guía CCN-STIC 817 Esquema Nacional de Seguridad - Gestión de Ciberincidentes, para clasificarlo de acuerdo con su tabla Criterios de determinación del nivel de impacto potencial. El nivel de impacto potencial de los ciberincidentes en la organización, será: Irrelevante, Bajo, Medio, Alto, Muy Alto y Crítico.

IV. Notificación obligatoria de los incidentes con nivel de impacto Alto, Muy alto y Crítico

IV.1 Las notificaciones efectuadas por las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad al Centro Criptológico Nacional (CCN), en el marco de la articulación de respuesta a los incidentes de seguridad y la prestación de servicios de respuesta por parte del Equipo de Respuesta a Incidentes de Seguridad del CCN-CERT, (Centro Criptológico Nacional - Computer Emergency Response Team) se realizará en los términos indicados en los artículos 36 y 37 del Real Decreto 3/2010, de 8 de enero.

IV.2 Para ello, se notificarán los incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada o los servicios prestados en relación con la categoría del sistema, determinada de acuerdo con lo dispuesto en los artículos 43, 44 y Anexo I del Real Decreto 3/2010, de 8 de enero. Se dice que un incidente tiene impacto significativo cuando, por su magnitud o características, impide el tratamiento de la información o los servicios prestados. A estos efectos, se considerará que tienen un impacto significativo los niveles Alto, Muy Alto y Crítico recogidos en la tabla Criterios de Determinación del Nivel de Impacto de la Guía CCN-STIC 817.

IV.3 En todo caso, serán de obligatoria notificación al CCN en el momento en que se produzcan, los incidentes de seguridad que por su nivel de impacto potencial sean calificados con el nivel de CRÍTICO, MUY ALTO o ALTO, mediante el empleo de las herramientas desarrolladas al efecto de la notificación de incidentes.

V. Evidencias a entregar en el caso de incidentes nivel Alto, Muy alto y Crítico

V.1 Tras la detección de un incidente de seguridad y con carácter inmediato se recopilarán evidencias del incidente, que serán documentadas y custodiadas de forma que se pueda determinar el modo de obtención, se garantice la cadena de custodia, y respetando el ordenamiento jurídico que resulte de aplicación. En la recolección y custodia de evidencia se aplicarán las recomendaciones establecidas al efecto en la Guía CCN-STIC 817.

V.2 De acuerdo con lo dispuesto en el artículo 37 del Real Decreto 3/2010, de 8 de enero, el CCN podrá recabar éstas y cualesquiera otras informaciones que se consideren relevantes para el análisis del incidente, así como los soportes informáticos que se estimen necesarios para la investigación, sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su normativa de desarrollo, así como la posible confidencialidad de datos de carácter institucional u organizativo.

VI. Obligación de remisión de estadísticas de incidentes

De conformidad con lo dispuesto en el artículo 24.2 del Real Decreto 3/2010, de 8 de enero, el registro de todos los incidentes de seguridad que se produzcan y de las acciones de tratamiento que se sigan, será utilizado para la mejora continua de la seguridad del sistema, a cuyo fin las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad elaborarán estadísticas de incidentes de seguridad que, al menos, con carácter anual, remitirán al CCN, incluyendo el resto de la antedicha información relativa a los incidentes.

VII. Notificación de impactos recibidos

Una vez determinado el impacto del ciberincidente y calificado como de carácter significativo a los efectos de lo establecido en el artículo 36 del ENS, será notificado al CCN en los términos previsto en el artículo IV de la presente Instrucción Técnica de Seguridad.

VIII. Desarrollo de herramientas automatizadas para facilitar las notificaciones

El CCN ha desarrollado la herramienta LUCIA, Listado Unificado de Coordinación de Incidentes y Amenazas) con el propósito de automatizar los mecanismos de notificación, comunicación e intercambio de información sobre incidentes de seguridad, de acuerdo a lo establecido en la Guía CCN-STIC 817. Esta herramienta se mantendrá permanentemente actualizada para atender dicho propósito.

IX. Régimen legal de las notificaciones y comunicación de información

Para la articulación de respuesta a los incidentes de seguridad y gestión de ciberincidentes a los que se refiere la presente Resolución, el suministro de información por las entidades del ámbito de aplicación de la presente Instrucción Técnica de Seguridad al CCN, motu proprio o a su requerimiento, se realizará teniendo en cuenta lo siguiente:

a) La comunicación de información que tenga la consideración de datos de carácter personal se efectuará con pleno cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y su normativa de desarrollo, atendiendo a que la comunicación de datos se realiza para el cumplimiento de fines directamente relacionados con la función legítima de las entidades cedentes y del CCN como cesionario, sin que sea preciso el consentimiento del afectado toda vez que tales datos han sido recabados para el ejercicio de las funciones propias de unos y otro, en los términos previstos en el artículo 6.2 de la citada Ley Orgánica.

Tampoco resultará de aplicación lo dispuesto en los párrafos uno y dos del artículo 5 de la reiterada Ley Orgánica, en base a lo dispuesto en su artículo 24.1, por afectar a la Ciberseguridad, como ámbito de especial interés para la Seguridad Nacional.

b) La comunicación de información de datos de carácter institucional u organizativo a la que se refiere el artículo 37.1.a) último párrafo, del Real Decreto 3/2010, de 8 de enero, será suministrada y comunicada en función de su confidencialidad, atendiendo a lo dispuesto en el artículo 43 y anexo I, en relación con el citado artículo 37.1.a) del ENS.

X. Disposición adicional

X.1 Las referencias contenidas en la presente Instrucción a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo se entenderán hechas, a partir del 25 de mayo de 2018, al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

X.2 Se añade un segundo párrafo al apartado VII de la Instrucción, con efectos a partir del 25 de mayo de 2018, con la siguiente redacción:

> «Cuando el incidente afecte a datos personales la notificación a la autoridad de control competente se realizará con independencia del nivel de impacto del incidente

en el Esquema Nacional de Seguridad. En aquellos casos en los que el impacto de un incidente o violación de la seguridad afecte a datos personales, la notificación se realizará según lo previsto en el artículo 33 del Reglamento General de Protección de Datos.»

X.3 La referencia contenida en el apartado IX, letra a), primer párrafo, de la Instrucción, al artículo 6.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se entenderá realizada, a partir del 25 de mayo de 2018, al artículo 6.1.c) del Reglamento General de Protección de Datos.

X.4 La referencia contenida en el apartado IX, letra a), segundo párrafo, a «los párrafos uno y dos del artículo 5 de la reiterada Ley Orgánica, en base a lo dispuesto en su artículo 24.1», se entenderá sustituida, a partir del 25 de mayo de 2018, por «el capítulo III del Reglamento General de Protección de Datos, en base a lo dispuesto en el artículo 23.1.a) del mismo».

§ 43

Orden PRE/3949/2006, de 26 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad

Ministerio de la Presidencia
«BOE» núm. 310, de 28 de diciembre de 2006
Última modificación: sin modificaciones
Referencia: BOE-A-2006-22786

Actualmente, en la mayoría de las relaciones de los ciudadanos con la Administración éstos deben presentar una fotocopia de su documento de identidad, ya sea su DNI, si se trata de un ciudadano español o su tarjeta equivalente para el caso de extranjeros residentes en territorio español.

Se estima que el número de fotocopias de documentos acreditativos de la identidad de un ciudadano presentadas anualmente en los trámites administrativos asciende a más de cuatro millones.

El 28 de abril de 2006, el Consejo de Ministros aprobó el Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

Los objetivos de dicha norma son, por un lado, suprimir la obligación de presentar fotocopias de los documentos acreditativos de identidad en todos los trámites administrativos, pudiendo sustituirse dicha fotocopia, en aquellos supuestos donde la constancia de los datos fuese imprescindible, por una consulta telemática a la Dirección General de la Policía y de la Guardia Civil de forma directa o diferida; y por otro dotar de mayor seguridad al método actual de verificación de la identidad de un ciudadano, ya que es más fácil manipular una fotocopia que suplantar la identidad del sistema de verificación de datos de identidad basado en la información preservada por la Dirección General de la Policía y de la Guardia Civil.

A partir de la puesta en funcionamiento de este sistema es el propio Departamento ante el que se solicita el trámite el encargado de comprobar, de oficio, la identidad del interesado. Esta consulta se realizará, en los casos en los que sea estrictamente necesario y tras obtener la autorización del interesado. La consulta se realizará con máximas garantías de seguridad y preservando la privacidad de los datos. En caso de que el interesado no dé su consentimiento a realizar esa consulta, deberá aportar su correspondiente fotocopia del Documento Nacional de Identidad.

El objeto de la presente Orden Ministerial es dar cumplimiento al mandato contenido en la disposición final primera del citado Real Decreto 522/2006, de 28 de abril, en virtud del cual el establecimiento de la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Identidad, así como la fecha en que dicho

sistema estará plenamente operativo, se llevará a cabo mediante orden, a propuesta conjunta de los Ministros del Interior y de Administraciones Públicas.

A tal fin, se han tenido en consideración las experiencias previas, las implicaciones técnicas, la búsqueda de racionalidad y sencillez de uso y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo respectivos informes favorables del Consejo Superior de Administración Electrónica y de la Agencia de Protección de Datos, a propuesta de los Ministros del Interior y de Administraciones Públicas, dispongo:

Primero.

Se aprueba el Reglamento Técnico del Sistema de Verificación de Datos de Identidad, que figura como anexo a la presente Orden Ministerial, como instrumento que establece la configuración, características, requisitos y procedimientos de acceso al citado Sistema.

Segundo.

Se fija como fecha de operatividad del Sistema de Verificación de Datos de Identidad el uno de enero de 2007, a partir de la cual no podrá exigirse por la Administración General del Estado o por los Organismos vinculados o dependientes de aquella la aportación de fotocopias del Documento Nacional de Identidad o de los documentos acreditativos de la identidad de extranjeros residentes en España o tarjeta equivalente, salvo en los supuestos previstos en el Real Decreto 522/2006, de 28 de abril.

Tercero.

La presente Orden Ministerial se aprueba en aplicación de lo dispuesto en la disposición final primera del Real Decreto 522/2006, de 28 de abril, por el que se suprime la aportación de fotocopias de documentos de identidad en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

Disposición final primera. *Aplicación y desarrollo.*

1. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio del Interior y previo informe del Consejo Superior de Administración Electrónica, se establecerán los parámetros de calidad de la prestación del servicio del Sistema de Verificación de Datos de Identidad y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial. A estos efectos, el Ministerio de Administraciones Públicas establecerá instrumentos de validación y vigilancia del cumplimiento de lo establecido en el párrafo anterior, sin perjuicio de las competencias de los Órganos de Control Interno.

2. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio del Interior y previo informe del Consejo Superior de Administración Electrónica, se podrá proceder a la actualización o modificación del Reglamento Técnico que se aprueba por la presente Orden Ministerial.

3. Se faculta a los Subsecretarios de los departamentos Ministeriales, a los Presidentes de los Organismos Públicos o a los responsables ministeriales correspondientes, para la adopción de las instrucciones o medidas que resulten adecuadas para garantizar el acceso y la utilización del Sistema de Verificación de Datos de Identidad por los órganos y unidades correspondientes a su ámbito.

Disposición final segunda. *Entrada en vigor.*

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Reglamento Técnico del Sistema de Verificación de Datos de Identidad

Primero. *Descripción del Sistema de Verificación de Datos de Identidad.*

El Sistema de Verificación de Datos de Identidad puesto a disposición de los Departamentos y Organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos del Documento de Identificación del Ciudadano custodiados por la Dirección General de la Policía y de la Guardia Civil en base a lo dispuesto en la Ley Orgánica 2/1986, de 13 de marzo, de Fuerzas y Cuerpos de Seguridad, que atribuye al Cuerpo Nacional de Policía, la función de expedición del Documento Nacional de Identidad y el control de entrada y salida del territorio nacional de españoles y extranjeros. Información que se encuentra registrada y custodiada en los ficheros de la Dirección General de la Policía y de la Guardia Civil, que soportan la gestión del documento nacional de identidad y la Tarjeta de Identificación de Extranjeros (Sus denominaciones, conforme a las Órdenes INT/1751/2002, de 20 de junio e INT/2190/2006, de 19 de junio, son ADDNIFIL y ADEXTTRA, respectivamente).

Segundo. *Adopción de medidas de seguridad, organizativas o técnicas de los organismos y aplicaciones que accedan al Sistema de Verificación de Datos de Identidad.*

1. Con carácter general los organismos que accedan al Sistema de Verificación de Datos de Identidad cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.
2. El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.
3. Lo dispuesto en esta Orden Ministerial se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el Reglamento de Medidas de Seguridad de los ficheros automatizados de datos de carácter personal aprobado por Real Decreto 994/1999, de 11 de junio.

Tercero. *Acceso al Sistema de Verificación de Datos de Identidad.*

1. El acceso al Sistema de Verificación de Datos de Identidad se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas, siguiendo el esquema de conexión que ésta tiene establecido para cualquier organismo público. Sólo en casos debidamente justificados y previa aprobación, por parte de la Secretaría del Consejo Superior de Administración Electrónica, de un plan para la ordenación de las comunicaciones se habilitarán temporalmente mecanismos de conexión alternativos.
2. El Sistema de Verificación de Datos de Identidad presentará dos formas alternativas de acceso para realizar las correspondientes consultas sobre la veracidad de ciertos datos de identidad:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto - HTTP/1.1 del IETF, donde un empleado público, debidamente acreditado e identificado, podrá realizar consultas con sólo disponer de un navegador con acceso al Sistema de Aplicaciones y Redes para las Administraciones Públicas y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los Organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

Cuarto. *Requisitos de autenticidad para el acceso al Sistema de Verificación de Datos de Identidad.*

1. Los accesos al Sistema de Verificación de Datos de Identidad se efectuarán utilizando certificados electrónicos reconocidos.

2. Los certificados electrónicos que se utilicen para identificarse ante el Sistema de Verificación de Datos de Identidad deberán ser certificados reconocidos que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997).

3. No podrán utilizarse certificados electrónicos caducados o revocados para acceder al Sistema de Verificación de Datos de Identidad.

Quinto. *Requisitos de confidencialidad del Sistema de Verificación de Datos de Identidad.*

1. El Sistema de Verificación de Datos de Identidad ofrecerá consultas en las que, a partir del Número del Documento de Identificación del Ciudadano o Extranjero, se devolverá el total, o un subconjunto, de los datos incorporados en dicho documento:

Nombre y apellidos del titular del documento.
Lugar y fecha de nacimiento.
Nombre de los padres.
Sexo.
Estado de vigencia del Documento.

El conjunto de datos a los que tenga acceso cada usuario del sistema será establecido, previa autorización y justificación, por parte del responsable en la Organización Administrativa.

2. Sólo organismos públicos debidamente autorizados tendrán acceso al Sistema de Verificación de Datos de Identidad. En todo organismo público existirá un responsable o administrador delegado del sistema que autorizará los accesos al Sistema de Verificación de Datos de Identidad.

3. Para realizar la consulta al Sistema de Verificación de Datos de Identidad, será preciso el consentimiento del interesado cuyos datos se vayan a verificar, salvo que una norma con rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento.

4. La consulta y el acceso a la información proporcionada por el Sistema de Verificación de Datos de Identidad deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta.

Sexto. *Requisitos de integridad de la información proporcionada por el Sistema de Verificación de Datos de Identidad.*

Todas las consultas que se realicen al Sistema de Verificación de Datos de Identidad, así como las respuestas que devuelva el propio sistema, deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el Sistema de Verificación de Datos de Identidad deba realizar a la Dirección General de la Policía y de la Guardia Civil, así cómo las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad de ambos organismos.

Séptimo. *Requisitos de disponibilidad de la información proporcionada por el Sistema de Verificación de Datos de Identidad.*

El Sistema de Verificación de Datos de Identidad estará disponible los 7 días de la semana las 24 horas del día.

Octavo. *Garantías jurídicas del Sistema de Verificación de Datos de Identidad ante posibles recursos.*

1. El servicio web proporcionado por este sistema sigue el estándar de intercambio de datos definido por «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

2. El Sistema de Verificación de Datos de Identidad dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de identidad realizadas, información de contexto asociada, como la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

3. Para certificar la fecha y tiempo de las actividades y sucesos registrados en el Sistema de Verificación de Datos de Identidad se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

4. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoría del Sistema de Verificación de Datos de Identidad.

Noveno. *Condiciones de la prestación del servicio.*

1. La gestión del Sistema de Verificación de Datos de Identidad corresponde al Ministerio de Administraciones Públicas.

2. Los organismos públicos que hagan uso de este servicio estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en esta Orden Ministerial.

3. Para poder acceder al Sistema de Verificación de Datos de Identidad, los Organismos Administrativos deberán designar a un responsable, tal y como se indica en el apartado segundo del punto quinto del presente anexo técnico, que será el encargado de autorizar a los accesos en su organismo. El nombramiento y cese de este responsable deberá ser comunicado al Ministerio de Administraciones Públicas, para la asignación de los permisos adecuados de acceso al sistema o la cancelación de los mismos.

§ 44

Orden PRE/4008/2006, de 27 de diciembre, por la que se establece la configuración, características, requisitos y procedimientos de acceso al Sistema de Verificación de Datos de Residencia

Ministerio de la Presidencia
«BOE» núm. 1, de 1 de enero de 2007
Última modificación: sin modificaciones
Referencia: BOE-A-2007-1

Actualmente, en la mayoría de las relaciones de los ciudadanos con la Administración, éstos deben indicar su lugar de residencia con un nivel de rigurosidad que varía desde la declaración expresa hasta la presentación de un certificado de empadronamiento expedido por el municipio en el cual están registrados sus datos de empadronamiento.

Se estima que el número de documentos acreditativos de la residencia expedidos anualmente asciende a más de diez millones de los cuales más de tres millones han sido solicitados, a su vez, por la Administración.

El 28 de abril de 2006, el Consejo de Ministros aprobó el Real Decreto 523/2006, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes.

Los objetivos de dicha norma son, por un lado, no exigir a quien tenga la condición de interesado en los procedimientos cuya tramitación y resolución corresponda a la Administración General del Estado o a los organismos públicos vinculados o dependientes de aquélla, la aportación del certificado de empadronamiento como documento acreditativo del domicilio y residencia; y por otro sustituir, en los procedimientos para cuya tramitación sea imprescindible acreditar de modo fehaciente los datos del domicilio y residencia del interesado, la presentación de documento acreditativo por una consulta electrónica mediante un Sistema de Verificación de Datos de Residencia puesto a disposición de los organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas y el Instituto Nacional de Estadística dependiente del Ministerio de Economía y Hacienda.

A partir de la puesta en producción de este sistema es el propio Departamento ante el que se solicita el trámite el encargado de comprobar, de oficio, la residencia del interesado. Esta consulta se realizará, en los casos en los que sea estrictamente necesario y tras obtener la autorización del interesado. La consulta se realizará con máximas garantías de seguridad y preservando la privacidad de los datos. En caso de que el interesado no dé su consentimiento a realizar esa consulta, deberá aportar el documento acreditativo de residencia que estime apropiado el organismo tramitador del expediente.

La presente Orden Ministerial tiene por objeto dar cumplimiento al mandato señalado en el Real Decreto 523/2006 de 28 de abril. A tal fin, se han tenido en consideración las

experiencias previas, las implicaciones técnicas, la búsqueda de racionalidad y sencillez de uso y el aprovechamiento de las ventajas de las economías de escala.

En su virtud, previo respectivos informes favorables del Consejo Superior de Administración Electrónica y de la Agencia Española de Protección de Datos, a propuesta de los Ministros de Economía y Hacienda y de Administraciones Públicas, dispongo:

Artículo único. *Objeto.*

1. Se aprueba el Reglamento Técnico del Sistema de Verificación de Datos de Residencia, que figura como anexo a la presente Orden Ministerial, como instrumento que establece la configuración, características, requisitos y procedimientos de acceso al citado Sistema.

2. Se fija como fecha de operatividad del Sistema de Verificación de Datos de Residencia la de entrada en vigor de la presente Orden, a partir de la cual no podrá exigirse en los procedimientos cuya tramitación y resolución corresponda a la Administración General del Estado, o a los Organismos vinculados o dependientes de aquélla, la aportación de certificados de empadronamiento, salvo en los supuestos previstos en el Real Decreto 523/2006, de 28 de abril.

3. La presente Orden Ministerial se aprueba en aplicación de lo dispuesto en la disposición final primera del Real Decreto 523/2006, de 28 de abril, por el que se suprime la exigencia de aportar el certificado de empadronamiento, como documento probatorio del domicilio y residencia, en los procedimientos administrativos de la Administración General del Estado y de sus organismos públicos vinculados o dependientes. Lo dispuesto en esta Orden Ministerial se aplicará en todo caso de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia.

Disposición final primera. *Aplicación y desarrollo.*

1. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio de Economía y Hacienda y previo informe del Consejo Superior de Administración Electrónica, se establecerán los parámetros de calidad de la prestación del servicio del Sistema de Verificación de Datos de Residencia y de cumplimiento de los requisitos y condiciones establecidas en la presente Orden Ministerial. A estos efectos, el Ministerio de Administraciones Públicas establecerá instrumentos de validación y vigilancia del cumplimiento de lo establecido en el párrafo anterior, sin perjuicio de las competencias de los Órganos de Control Interno.

2. Mediante Resolución de la Secretaría General para la Administración Pública del Ministerio de Administraciones Públicas, con la conformidad del Ministerio de Economía y Hacienda y previo informe del Consejo Superior de Administración Electrónica, se podrá proceder a la actualización o modificación del Reglamento Técnico que se aprueba por la presente Orden Ministerial.

3. Se faculta a los Subsecretarios de los departamentos Ministeriales, a los Presidentes de los Organismos Públicos o a los responsables ministeriales correspondientes, para la adopción de las instrucciones o medidas que resulten adecuadas para garantizar el acceso y la utilización del Sistema de Verificación de Datos de Residencia por los órganos y unidades correspondientes a su ámbito.

Disposición final segunda. *Entrada en vigor.*

La presente Orden Ministerial entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Reglamento Técnico del Sistema de Verificación de Datos de Residencia

Primero. Descripción del Sistema de Verificación de Datos de Residencia.

El Sistema de Verificación de Datos de Residencia puesto a disposición de los Departamentos y Organismos de la Administración General del Estado por parte del Ministerio de Administraciones Públicas se establece como servicio horizontal para la consulta y comprobación de los datos sobre residencia de los ciudadanos mediante el acceso a los Padrones municipales coordinados por el Instituto Nacional de Estadística, en base a lo dispuesto en la Ley 7/1985, de 2 de abril, reguladora de las Bases de Régimen Local, en relación con el Padrón Municipal, en la que se atribuye al Instituto Nacional de Estadística, entre otras, la función de coordinación de los distintos padrones municipales. Ésta información se encuentra registrada y custodiada en los ficheros del Instituto Nacional de Estadística registrados en la Agencia de Protección de Datos con la denominación «PADRONES MUNICIPALES», conforme a la Orden ECO/143/2002, de 10 de enero, publicada en el BOE 26, de 30 de enero de 2002.

Segundo. Adopción de medidas de seguridad, organizativas o técnicas del acceso al Sistema de Verificación de Datos de Residencia.

1. Con carácter general los organismos que accedan al Sistema de Verificación de Datos de Residencia cumplirán con las medidas de seguridad, conservación y normalización que se detallan en los Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades aprobados por el Consejo Superior de Administración Electrónica mediante Resolución de 26 de mayo de 2003 y revisiones posteriores.

2. El alcance e intensidad de aplicación de las medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) del Consejo Superior de Administración Electrónica.

3. Lo dispuesto en esta Orden Ministerial se aplicará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y demás normativa aplicable en esta materia como el Reglamento de Medidas de Seguridad de los ficheros automatizados de datos de carácter personal aprobado por Real Decreto 994/1999, de 11 de junio.

Tercero. Acceso al Sistema de Verificación de Datos de Residencia.

1. El acceso al Sistema de Verificación de Datos de Residencia se realizará a través del Sistema de Aplicaciones y Redes para las Administraciones Públicas, siguiendo el esquema de conexión que ésta tiene establecido para cualquier departamento u organismo público. Sólo en casos debidamente justificados y previa aprobación, por parte de la Secretaría del Consejo Superior de Administración Electrónica, de un plan para la ordenación de las comunicaciones se habilitarán temporalmente mecanismos de conexión alternativos.

2. El Sistema de Verificación de Datos de Residencia presentará dos formas de acceso para realizar las correspondientes consultas sobre el lugar de domicilio y residencia de un ciudadano:

Un interfaz accesible a través de un navegador de Internet, conforme al RFC 2616: Protocolo de Transferencia de Hipertexto – HTTP/1.1 o superior, del IETF, donde un empleado público, debidamente acreditado e identificado, podrá realizar consultas con sólo disponer de un navegador con acceso al Sistema de Aplicaciones y Redes para las Administraciones Públicas y firma electrónica.

Un interfaz automatizado de servicio web, conforme al estándar WSDL 1.1 o superior del W3C cuya definición inicial, y sucesivas actualizaciones, serán puestas a disposición de los departamentos y organismos a través del Consejo Superior de Administración Electrónica y su Comisión Permanente.

Cuarto. Requisitos de autenticidad para el acceso al Sistema de Verificación de Datos de Residencia.

1. Los accesos al Sistema de Verificación de Datos de Residencia se efectuarán utilizando certificados electrónicos reconocidos.

2. Los certificados electrónicos que se utilicen para identificarse ante el Sistema de Verificación de Datos de Residencia deberán ser certificados reconocidos que cumpla la recomendación UIT X.509 versión 3 o superiores (ISO/IEC 9594-8 de 1997).

3. No podrán utilizarse certificados electrónicos caducados o revocados para acceder al Sistema de Verificación de Datos de Residencia.

Quinto. Requisitos de confidencialidad del Sistema de Verificación de Datos de Residencia.

1. El Sistema de Verificación de Datos de Residencia, a partir del Número del Documento de Identificación del Ciudadano y/o de un conjunto de datos personales suficientes para identificar unívocamente al mismo, devolverá el total, o un subconjunto de los datos referentes al domicilio y residencia asociados a un ciudadano:

Provincia.
Municipio.
Entidad Colectiva.
Entidad Singular.
Núcleo.
Dirección (Via, Kmt, Número, Número Superior, Bloque, Portal, Escalera, Planta, Puerta).

El conjunto de datos a los que tenga acceso cada usuario del sistema será establecido, previa autorización y justificación, por parte del responsable en la Organización Administrativa.

En caso de que los datos introducidos no fueran suficientes para identificar de manera única a un ciudadano el sistema no devolverá en la respuesta información sobre ningún ciudadano.

2. Sólo organismos públicos debidamente autorizados tendrán acceso al Sistema de Verificación de Datos de Residencia. En todo organismo público existirá un responsable o administrador delegado del sistema que autorizará los accesos al Sistema de Verificación de Datos de Residencia.

3. Para realizar la consulta al Sistema de Verificación de Datos de Residencia, será preciso el consentimiento del interesado cuyos datos se vayan a consultar, salvo que una norma de rango de ley autorice dicha consulta. Dicho consentimiento deberá constar en la solicitud de iniciación del procedimiento, o en cualquier otra comunicación posterior, siempre y cuando dicha comunicación sea previa a la consulta en el sistema, no pudiendo realizarse consulta alguna en caso de no contar con el consentimiento de forma fehaciente. Los impresos o formularios electrónicos de solicitudes de iniciación de procedimientos administrativos deberán adecuarse para recoger dicho consentimiento.

4. La consulta y el acceso a la información proporcionada por el Sistema de Verificación de Datos de Residencia deberá realizarse con una finalidad concreta, que quedará recogida en el momento de la consulta.

Sexto. Requisitos de integridad de la información proporcionada por el Sistema de Verificación de Datos de Residencia.

Todas las consultas que se realicen al Sistema de Verificación de Datos de Residencia, así como las respuestas que devuelva el propio sistema, deberán haber sido firmadas electrónicamente. Esta firma electrónica tiene por objeto garantizar tanto la integridad de los datos intercambiados como la identidad de las partes que intervienen y el no repudio de la consulta.

De la misma forma, todas las consultas que el Sistema de Verificación de Datos de Residencia deba realizar al Instituto Nacional de Estadística o a otros organismos con capacidad de informar sobre la residencia de los ciudadanos, así cómo las correspondientes respuestas obtenidas resultado de las mismas, habrán de ser debidamente firmadas electrónicamente para garantizar tanto la integridad de la información como la identidad de ambos organismos.

Séptimo. Requisitos de disponibilidad de la información proporcionada por el Sistema de Verificación de Datos de Residencia.

El Sistema de Verificación de Datos de Residencia estará disponible los 7 días de la semana las 24 horas del día.

Octavo. Garantías jurídicas del Sistema de Verificación de Datos de Residencia ante posibles recursos.

1. El servicio web proporcionado por este sistema sigue el estándar de intercambio de datos definido por la iniciativa «Sustitución de Certificados en Soporte Papel» del Consejo Superior de Administración Electrónica, que reúne, en base a la normativa vigente, las garantías jurídicas aplicables al intercambio de datos entre Administraciones Públicas.

2. El Sistema de Verificación de Datos de Residencia dispondrá de un módulo de auditoría, en el que quedarán registradas todas las consultas de datos de residencia realizadas, información de contexto asociada, la identidad del solicitante, la fecha y la finalidad de la consulta, y aquellos eventos relevantes desencadenados a partir de la propia consulta. Se garantizará la integridad y no repudio de la información registrada mediante técnicas de firma electrónica y sellado de tiempo, estableciéndose, asimismo, medidas técnicas para garantizar la disponibilidad y recuperación de aquella información que no se mantenga on-line por motivos de eficiencia técnica o seguridad.

3. Para certificar la fecha y tiempo de las actividades y sucesos registrados en el Sistema de Verificación de Datos de Residencia se hará uso del Servicio de Sellado de Tiempo de la Plataforma de Firma Electrónica del Ministerio de Administraciones Públicas, sincronizada con el Real Instituto y Observatorio de la Armada, de conformidad con lo previsto sobre la hora legal en el Real Decreto 1308/1992, de 23 de octubre, por el que se declara el Laboratorio de la Armada como laboratorio depositario del patrón nacional de Tiempo y laboratorio asociado al centro Español de Metrología, y según las condiciones técnicas y protocolos que el citado Organismo establezca.

4. Sólo personal de la Administración Pública debidamente autorizado y acreditado podrá acceder a las funcionalidades de auditoria del Sistema de Verificación de Datos de Residencia.

Noveno. Condiciones de la prestación del servicio.

1. La gestión del Sistema de Verificación de Datos de Residencia corresponde al Ministerio de Administraciones Públicas.

2. Los organismos públicos que hagan uso de este servicio estarán sujetos a las medidas de seguridad, los requisitos de autenticidad, integridad, confidencialidad, disponibilidad y criterios técnicos establecidos en esta Orden Ministerial.

3. Para poder acceder al Sistema de Verificación de Datos de Residencia, los Organismos Administrativos deberán designar a un responsable, tal y como se indica en el apartado segundo del punto quinto del presente anexo técnico, que será el encargado de autorizar los accesos en su organismo. El nombramiento y cese de este responsable deberá ser comunicado al Ministerio de Administraciones Públicas, para la asignación de los permisos adecuados de acceso al sistema o la cancelación de los mismos.

§ 45

Orden EHA/1307/2005, de 29 de abril, por la que se regula el empleo de medios electrónicos en los procedimientos de contratación

Ministerio de Economía y Hacienda
«BOE» núm. 114, de 13 de mayo de 2005
Última modificación: sin modificaciones
Referencia: BOE-A-2005-7774

La implantación de un efectivo y fiable sistema de administración electrónica que se extienda a todas las esferas de la actividad administrativa constituye uno de los principales retos que ha de afrontar la Administración de cara a definir un nuevo sistema, más eficaz y transparente, de relaciones con los ciudadanos.

Ya la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, promulgada en un momento en que las tecnologías de la información y de la comunicación comenzaban un desarrollo que se aceleraría en el transcurso de la década, anticipó la necesidad de insertar plenamente estos nuevos instrumentos en la actividad administrativa instando, desde su artículo 45, a las Administraciones Públicas para que promuevan la incorporación de técnicas electrónicas, informáticas y telemáticas en el desarrollo de su actividad y en el ejercicio de sus competencias. En igual sentido, la reforma de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común efectuada por la Ley 24/2001, de 27 de diciembre, de medidas Fiscales, Administrativas y del Orden Social, tuvo por finalidad potenciar el uso de medios electrónicos, informáticos y telemáticos por la Administración.

Las previsiones de la Ley 30/1992 fueron desarrolladas por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias y documentos y devolución de originales y el régimen de las oficinas de registro, ambos modificados por el Real Decreto 209/2003, de 21 de febrero, por el que se regulan los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos, normas que, en conjunción con sus antecedentes legales, constituyen la base general para el uso de medios electrónicos en el ámbito administrativo.

Sobre este base general, la presente Orden viene a regular, al amparo de la disposición adicional décima del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por Real Decreto 1098/2001, de 12 de octubre, las especialidades del uso de los medios electrónicos en el procedimiento de contratación, cuya particular consideración frente al resto de procedimientos administrativos, por razón de su peculiar naturaleza, viene reconocida por la disposición adicional séptima del texto refundido de la

Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio. En la redacción de la Orden, por otra parte, se han tenido particularmente en cuenta las directrices de la Directiva 2004/18/CE, del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios, de la que constituyen una parte esencial las provisiones dirigidas a introducir sistemas efectivos de licitación electrónica en la contratación pública europea.

Desde un punto de vista práctico, la contratación administrativa es un ámbito en el que la correcta implantación de medios electrónicos puede producir especiales beneficios, para la Administración y para los operadores económicos, generando importantes ahorros de tiempo y costes y contribuyendo decisivamente a incrementar el nivel de competencia, transparencia y control. Por ello, se considera urgente incorporar las tendencias antes apuntadas sobre tramitación telemática de los expedientes administrativos al ámbito de la contratación, sentando las bases normativas que posibiliten la articulación, a corto plazo, de sistemas electrónicos en esta área de actividad; ello permitirá generar la necesaria experiencia en la aplicación de las nuevas tecnologías de la información y de la comunicación a los procedimientos legales de contratación que, eventualmente, podría servir de base a una revisión más profunda de su configuración, todo ello sin renunciar a la deseable homologación de soluciones cuando se desarrollen y adopten de forma mayoritaria estándares europeos para la contratación electrónica.

Ha de señalarse, por último, que a pesar del carácter de norma básica que tiene la disposición adicional décima del Reglamento General de la Ley de Contratos de las Administraciones Públicas, base jurídica de la presente Orden, ésta limita su eficacia al ámbito estatal, por estimarse preferible esperar a que se decanten suficientemente las medidas de implementación del marco normativo constituido por la Directiva 2004/18/CE que, impulsadas desde instancias comunitarias, se dirigen a estandarizar los sistemas y aplicaciones utilizados en la licitación electrónica para garantizar su interoperabilidad y el intercambio de datos entre las Administraciones europeas, y a que se consolide suficientemente una experiencia en el empleo de estos medios que permita identificar con mayor seguridad aquellos extremos de la contratación electrónica cuya homogeneidad deba garantizarse mediante su regulación por disposiciones de carácter básico.

En su virtud, previo informe de la Junta Consultiva de Contratación Administrativa y con la aprobación del Ministro de Administraciones Públicas, dispongo:

Primero. *Objeto y ámbito de aplicación.*

La presente Orden tiene por objeto regular, al amparo de lo dispuesto en la disposición adicional décima del Reglamento General de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto 1098/2001, de 12 de octubre, la utilización de medios electrónicos en los procedimientos de contratación sujetos a las prescripciones del texto refundido de la Ley de Contratos de las Administraciones Públicas, aprobado por el Real Decreto Legislativo 2/2000, de 16 de junio, que se tramiten por la Administración General del Estado, sus Organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social y demás entidades públicas estatales, así como por las sociedades de derecho privado vinculadas a las anteriores.

Segundo. *Condiciones para el empleo de medios electrónicos en los procedimientos de contratación.*

Uno. Podrán utilizarse medios electrónicos en los procedimientos de contratación siempre que en los pliegos de cláusulas administrativas particulares se haya establecido su admisibilidad. A estos efectos, los pliegos deberán indicar los trámites que, en su caso, puedan ser cumplimentados por vía electrónica, informática o telemática, y los medios electrónicos y sistemas de comunicación y notificación utilizables, que deberán ajustarse a las especificaciones detalladas en el apartado tercero de esta Orden.

En estos supuestos, los pliegos y la restante documentación necesaria para tomar parte en la licitación deben estar disponibles para los interesados en forma electrónica, en un formato conforme con los estándares abiertos aplicables a cada documento, y ser accesibles a través de procedimientos electrónicos de carácter no discriminatorio, de acceso público, y

compatibles con las tecnologías de la información y de la comunicación de uso general. En el caso de que el medio de difusión elegido sea Internet el formato de dichos documentos deberá ser conforme con las Recomendaciones aplicables aprobadas por el World Wide Web Consortium (W3C).

Dos. Cuando, conforme a lo señalado en el punto anterior, los pliegos hayan admitido el empleo de medios electrónicos, informáticos o telemáticos en el procedimiento de contratación, su uso será potestativo para los licitadores.

El licitador que desee utilizar estos medios en sus relaciones con el órgano de contratación deberá presentar por vía electrónica su proposición o solicitud de participación y la documentación que, según el pliego, pueda remitirse en esta forma y manifestar expresamente, al mismo tiempo, que opta por el empleo de medios electrónicos para la presentación de escritos, comunicaciones y documentos y para la recepción de notificaciones, a cuyo efecto debe estar dado de alta en un sistema de notificación telemática admitido por el órgano de contratación en el pliego y disponer de una dirección electrónica, con los requisitos indicados en el numero cinco del apartado tercero de esta Orden.

La opción por el uso de medios electrónicos vincula al licitador durante toda la fase de licitación del contrato y, si llegara a ser el adjudicatario del mismo, durante el período de su ejecución, constituyéndole en la obligación de utilizar los programas, formatos y aplicaciones establecidos, salvo que causas técnicas, debidamente acreditadas, lo impidan.

En ningún caso podrá derivarse para los licitadores y contratistas una discriminación o restricción de cualquier naturaleza contraria a los principios de libre concurrencia e igualdad de trato por razón de los medios por los que opten para efectuar sus comunicaciones con el órgano de contratación.

Tres. No obstante lo señalado en el número anterior, en los contratos en que, por razón del número previsible de licitadores, por la cantidad y características de los productos o bienes objeto de licitación, o por la concurrencia de otras peculiaridades debidamente motivadas, se considere conveniente por razones de agilidad y simplificación del procedimiento y, en todo caso, en las licitaciones y contratos que se celebren dentro del sistema de adquisición centralizada de bienes y servicios al amparo de los artículos 183 y 199 de la Ley de Contratos de las Administraciones Públicas, los pliegos de cláusulas administrativas podrán establecer la necesidad de que la presentación de las solicitudes de participación y proposiciones, la aportación de documentos y las comunicaciones y notificaciones entre el órgano de contratación y los licitadores o contratistas, se realicen, en todas o en alguna de sus fases, de forma exclusiva, por medios electrónicos.

Para que en los pliegos pueda establecerse la necesaria utilización de medios electrónicos, deberá acreditarse en el expediente de contratación, que esta exigencia no supondrá restricción o discriminación alguna para los licitadores, en el sentido señalado en la disposición adicional decimoctava de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Tercero. *Requisitos y especificaciones técnicas de los medios electrónicos utilizables en la contratación administrativa.*

Uno. Con carácter general se aplicarán a los dispositivos y aplicaciones de registro, notificación y de la prestación del servicio de dirección electrónica las medidas de seguridad, conservación y normalización que se detallan en los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» aprobados por el Consejo Superior de Informática y para el impulso de la Administración Electrónica y accesibles en su sitio web.

Dichas medidas de seguridad, conservación y normalización vendrán determinadas por el resultado del análisis y gestión de riesgos que se realice, recomendándose a estos efectos la utilización de la metodología Magerit.

Dos. Los sistemas de comunicaciones y para el intercambio y almacenamiento de información deberán garantizar la integridad de los datos y la confidencialidad de las ofertas y solicitudes de participación.

Los medios electrónicos utilizables en los procedimientos de contratación no podrán ser discriminatorios, y deberán ser de acceso público y compatibles con las tecnologías de la

información y de la comunicación de uso general, de forma que no se restrinja indebidamente el acceso de los operadores económicos al procedimiento de adjudicación.

Tres. La información, las especificaciones técnicas, y los programas y aplicaciones necesarios para la presentación electrónica de las ofertas y solicitudes de participación deberán estar a disposición de todas las partes interesadas.

Cuatro. Los formatos que el órgano de contratación declare admisibles en los pliegos para la aportación de documentos electrónicos deberán ser conformes a los estándares abiertos que se especifican en el anexo de esta norma.

Cinco. Los medios electrónicos que se utilicen en el procedimiento de contratación deben poder garantizar, de forma razonable en función del estado de la técnica, el cumplimiento de los siguientes requerimientos:

a) Que la firma electrónica reconocida exigida por el número dos del apartado cuarto de esta Orden se ajusta a las disposiciones de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

b) Que sólo los órganos competentes, en la fecha señalada para ello, pueden tener acceso a los datos transmitidos o que en caso de violación de la prohibición de acceso, esta violación pueda detectarse con claridad.

c) Que se deje un rastro de auditoría que permita el control posterior de las transacciones efectuadas.

Seis. El sistema de notificación telemática que se utilice deberá acreditar la fecha y hora en que se produzcan la recepción de la notificación en la dirección electrónica asignada al interesado y el acceso de éste al contenido del mensaje, así como poner de manifiesto cualquier incidencia técnica que imposibilite el cumplimiento de lo anterior. Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran diez días naturales sin que se acceda a su contenido se entenderá que la notificación ha sido rechazada.

La dirección electrónica asignada al licitador deberá cumplir los siguientes requisitos:

a) Poseer identificadores de usuario y claves de acceso para garantizar la exclusividad de su uso,

b) contar con mecanismos de autenticación que garanticen la identidad del usuario, y

c) contar con mecanismos para proteger la confidencialidad de los datos.

Siete. Atendiendo al grado de desarrollo y consolidación de los trabajos de normalización internacional, los documentos electrónicos que se utilicen en el procedimiento de contratación deberán adaptarse a la nomenclatura y estándares adoptados en el seno del programa para la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y ciudadanos (programa IDA/IDABC) en relación con las compras electrónicas o en su caso a otros estándares internacionales de carácter abierto.

Cuarto. *Régimen de las comunicaciones y notificaciones telemáticas.*

Uno. En todo lo no previsto en esta Orden, la validez y los efectos jurídicos de las comunicaciones y de las notificaciones telemáticas se regirán por lo establecido en el artículo 59 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, y en el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias y documentos y devolución de originales y el régimen de las oficinas de registro, modificado por el Real Decreto 209/2003, de 21 de febrero.

Dos. Todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos y se emitan tanto en la fase preparatoria como en las fases de licitación, adjudicación y ejecución del contrato deben ser autenticados mediante una firma electrónica reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Tres. Las aplicaciones que se utilicen para efectuar las comunicaciones, notificaciones y envíos documentales entre el licitador o contratista y el órgano de contratación deben permitir acreditar la fecha y hora de su emisión o recepción, su contenido y el remitente y destinatario de las mismas. En especial, estas aplicaciones deben garantizar que se deja constancia de la hora y la fecha exactas de la recepción de las proposiciones o solicitudes de participación y de cuanta documentación deba presentarse ante el órgano de contratación.

Cuatro. En los documentos, comunicaciones y notificaciones telemáticas deberá usarse el juego de caracte-res ISO/IEC-8859-1 («latin alphabet -1»).

Cinco. Las proposiciones o solicitudes de participación, así como la documentación que se presente se enviarán libres de virus informáticos que dificulten o imposibiliten su lectura, siendo responsabilidad de los licitadores velar por el cumplimiento de esta previsión. No obstante, la mera presencia de virus en tales documentos no determinará, por sí sola, su exclusión de la licitación siempre que sea posible acceder a su contenido esencial y que resulte indubitable que los términos de la oferta no han sido alterados por efecto del virus.

Quinto. *Transmisión electrónica de datos entre órganos administrativos.*

Uno. Los órganos de contratación podrán recabar los datos y los documentos referentes a la empresa que, de conformidad con lo establecido en el artículo 79 de la Ley de Contratos de las Administraciones Públicas, requiera el pliego de cláusulas administrativas, especialmente los correspondientes a su capacidad y solvencia, de los órganos y registros de las Administraciones y Entidades públicas mediante interconexión electrónica con sus bases de datos y documentales, si el licitador o su representante así lo solicitan, indicando el lugar en que dichos datos y documentos consten o se encuentren, y siempre que, con arreglo a las normas vigentes, sea posible reconocer eficacia jurídica a los mismos, con respeto, en todo caso, a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Dos. Los registros de licitadores de la Administración General del Estado, sus Organismos autónomos, entidades gestoras y servicios comunes de la Seguridad Social y demás entidades públicas estatales facilitarán por medios electrónicos a los órganos y a las mesas de contratación dependientes de cualquiera de ellas que así lo requieran, certificaciones sobre la personalidad, capacidad de obrar y representación de las empresas inscritas, en la forma y con los efectos previstos en la Orden HAC/664/2004, de 9 de marzo, por la que se establecen los mecanismos de coordinación entre los registros voluntarios de licitadores.

Asimismo, con la autorización de las empresas inscritas y mediante el oportuno convenio de colaboración basado en el principio de reciprocidad, estos certificados electrónicos podrán ser facilitados a otras Administraciones Públicas, a los efectos de la participación de las empresas en sus propios procedimientos de contratación.

Sexto. *Apertura de proposiciones.*

Uno. En los casos en que el órgano de contratación establezca en los pliegos la necesidad de que las proposiciones se presenten cifradas, una vez realizadas las actuaciones previstas en los artículos 81 y 82 del Reglamento General de la Ley de Contratos de las Administraciones Públicas y en el acto público a que se refiere el artículo 83, deberá procederse, en primer término, a descifrar los ficheros que contengan la documentación correspondiente.

Dos. En el caso de que no pueda descifrarse alguno de los ficheros presentados, se rechazará la proposición si ello fuese debido a una causa imputable al licitador. Si por causas no imputables al licitador, surgieran circunstancias que impidieran el desciframiento, se suspenderá el acto hasta que por la mesa de contratación pueda subsanarse la incidencia de conformidad con lo previsto en el Reglamento General de la Ley de Contratos de las Administraciones Públicas, en cuyo momento se reanudará el mismo.

Séptimo. *Coordinación de los sistemas.*

Los sistemas de notificación y registro a los que se refiere la presente orden se coordinarán adecuadamente con los que, en su caso, se creen al amparo de lo dispuesto en el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado y en el Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, modificado por el Real Decreto 209/2003, de 21 de febrero.

Octavo. *Instrucciones.*

El Director General del Patrimonio del Estado dictará las instrucciones que resulten precisas para facilitar la adaptación a los estándares y nomenclatura a los que se refiere el número siete del apartado tercero de la presente orden, que garanticen la compatibilidad e interoperabilidad de los sistemas de información y comunicación que intervienen en los procesos de contratación electrónica, pudiendo, a estos efectos, modificar el anexo de esta Orden con el fin de incluir nuevos formatos que cumplan con los requisitos exigidos.

Noveno. *Regulación del uso de medios electrónicos en los procedimientos de contratación centralizada de bienes y servicios.*

En los procedimientos de contratación centralizada de bienes y servicios, las condiciones de uso de medios electrónicos podrán regularse, con arreglo a lo establecido en esta Orden, además de en los pliegos de cláusulas administrativas particulares, por resolución del Director General del Patrimonio del Estado.

Décimo. *Modificación del Anexo VII del Reglamento General de la Ley de Contratos de las Administraciones Públicas.*

Haciendo uso de la habilitación conferida por la disposición adicional sexta del Reglamento General de la Ley de Contratos de las Administraciones Públicas, se modifican los modelos de anuncios del anexo VII del dicho Reglamento que a continuación se indican, en el siguiente sentido:

En el modelo B), «Modelo de anuncio para la licitación de los contratos de obras», se añadirá un apartado con la siguiente redacción:

«14. En su caso, sistema de notificación telemática aplicable.»

En el modelo C), «Modelo de anuncio para la licitación de los contratos de gestión de servicios públicos», se añadirá un apartado con la siguiente redacción:

«13. En su caso, sistema de notificación telemática aplicable.»

En el modelo D), «Modelo de anuncio para la licitación de los contratos de suministro», se añadirá un apartado con la siguiente redacción:

«14. En su caso, sistema de notificación telemática aplicable.»

En el modelo E), «Modelo de anuncio para la licitación de los contratos de consultoría y asistencia y de servicios», se añadirá un apartado con la siguiente redacción:

«14. En su caso, sistema de notificación telemática aplicable.»

En el modelo F), «Modelo de anuncio para la licitación de los contratos administrativos especiales», se añadirá un apartado con la siguiente redacción:

«13. En su caso, sistema de notificación telemática aplicable.»

Undécimo. *Entrada en vigor.*

Uno. La presente Orden entrará en vigor a los dos meses de su publicación en el Boletín Oficial del Estado salvo lo dispuesto en el apartado noveno que entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

Dos. No obstante, durante un plazo de dos años a partir de la entrada en vigor de la presente Orden, los órganos de contratación podrán seguir empleando los formatos para el intercambio de datos que estén usando, siempre que respondan a estándares comúnmente aceptados y que su uso no sea contrario a los principios de libertad de acceso y no discriminación.

ANEXO

Formatos admisibles para los documentos intercambia-dos en los procesos de contratación electrónica

1. Formatos de datos estructurados.

1.1 Formato de documentos de datos: XML.
Estándar aplicable: XML 1.1 (Recomendación del W3C, 4 de febrero de 2004).
1.2 Formato de documentos de validación: XML Schema Language.
Estándar aplicable: XML Schema Language 1.1 (Recomendación del W3C, 2 de mayo de 2001).

2. Formato de documentos de texto y documentos compuestos: ISO-HTML.
Estándar aplicable: ISO/IEC 15445.

3. Formatos de gráficos e imágenes:

a) Formato: JPEG.
Estándar aplicable: ISO/IEC 10918.
b) Formato: TIFF.
Estándar aplicable: ISO/IEC 12234.
c) Formato: PNG.
Estándar aplicable: ISO/IEC 15948.
d) Formato: CGM.
Estándar aplicable: ISO/IEC 12071.

§ 46

Orden EHA/1220/2008, de 30 de abril, por la que se aprueban las instrucciones para operar en la Plataforma de Contratación del Estado

Ministerio de Economía y Hacienda
«BOE» núm. 105, de 1 de mayo de 2008
Última modificación: sin modificaciones
Referencia: BOE-A-2008-7708

La Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, con el fin de fomentar la transparencia de la actividad contractual del sector público, regula el Perfil de Contratante como medio preferente de difusión de tal información, basado en el Perfil de Comprador previsto en la Directiva 2004/18/CE, de 31 de marzo de 2004, sobre coordinación de los procedimientos de adjudicación de los contratos públicos de obras, de suministro y de servicios. Así, el artículo 42 de la Ley 30/2007 prevé que los órganos de contratación harán accesible a través de Internet su Perfil de Contratante, el cual podrá incluir cualesquiera datos e informaciones referentes a la actividad contractual del órgano de contratación, además de los aspectos que la Ley de Contratos del Sector Público establece como de necesaria publicación.

El artículo 309 de la Ley 30/2007 señala que la Junta Consultiva de Contratación Administrativa del Estado pondrá a disposición de todos los órganos de contratación del sector público una plataforma electrónica que permita dar publicidad a las convocatorias de licitaciones, a sus resultados y al resto de información contractual considerada relevante. La Plataforma de Contratación del Estado sirve así de espacio virtual de contacto entre los órganos de contratación del sector público y los interesados, pudiendo estos últimos acceder a la misma a través de un portal único.

En la Plataforma de Contratación del Estado se publicarán necesariamente los perfiles de contratante de los órganos de contratación de la Administración General del Estado, sus Organismos autónomos, Entidades gestoras y Servicios Comunes de la Seguridad Social y demás Entidades públicas estatales. Voluntariamente, además, se publicarán en esta Plataforma los perfiles de contratante de los restantes entes del sector público estatal y de los órganos de contratación de las Comunidades Autónomas y las Entidades Locales.

Además de la publicación voluntaria de los perfiles de contratante de los órganos de contratación de las Comunidades Autónomas y de las Entidades locales, la Plataforma de Contratación del Estado se interconectará con los servicios de información similares que articulen esas Administraciones Territoriales en la forma que determinen los convenios que se concluyan al efecto.

Para la operatividad de la Plataforma, resulta necesario establecer las directrices para que los órganos de contratación y demás órganos con competencias en materia de contratos públicos puedan proceder a publicar la información relevante a través de la Plataforma, así como definir las especificaciones CODICE que se utilizarán en la Plataforma. Todo ello sin

perjuicio que éstos documentos no puedan ser utilizados en la tramitación de expedientes de gasto a efectos de fiscalización previa, hasta que no se produzca la correspondiente adaptación de los sistemas orientados al control prevista para el 1 de junio de 2008.

En virtud de lo anterior, en ejercicio de las competencias atribuidas por el apartado 2 de la disposición final novena de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, dispongo:

CAPÍTULO I

Disposiciones Generales

Artículo 1. *Puesta en funcionamiento y dirección en INTERNET.*

La Plataforma de Contratación del Estado estará operativa a partir del día 2 de mayo de 2008, siendo accesible en la dirección http://www.contrataciondelestado.es,

En la Plataforma podrán publicar su Perfil de Contratante los órganos de contratación con competencias originarias, delegadas o desconcentradas, en la forma regulada en el capítulo II.

En todo caso, los órganos de contratación de la Administración General del Estado, sus Organismos autónomos, Entidades gestoras y Servicios comunes de la Seguridad Social y demás Entidades públicas estatales deberán publicar en esta plataforma su Perfil de Contratante.

Igualmente, podrán publicar información contractual la Junta Consultiva de Contratación Administrativa del Estado y los organismos similares de las Comunidades Autónomas, así como los órganos con competencias en materia de ordenación de la contratación pública, de acuerdo con lo previsto en el capítulo III.

Artículo 2. *Aprobación de especificaciones técnicas.*

Las especificaciones de contenidos y formatos serán las correspondientes a la arquitectura de información CODICE que se detalla en el Anexo III.

Las especificaciones de los protocolos de comunicación serán las recogidas en el Anexo IV.

CAPÍTULO II

Publicación del Perfil de Contratante en la Plataforma de Contratación del Estado

Artículo 3. *Alta del Perfil de Contratante.*

El alta del Perfil de Contratante deberá solicitarse por el titular de los órganos de contratación unipersonales, o por el Presidente en el caso de órganos de contratación de carácter colegiado, remitiendo a la Subdirección General de Coordinación de la Contratación Electrónica la correspondiente petición acompañada del formulario contenido en el anexo I debidamente cumplimentado.

A la solicitud se acompañará la documentación que acredite la competencia para contratar del órgano de contratación (norma legal o reglamentaria o disposición estatutaria, donde figure atribuida la facultad de celebrar contratos, normas de delegación o desconcentración de competencias —en el caso de que se trate de órganos administrativos o de entes, organismos o entidades de derecho público—, o poderes otorgados —cuando se trate de órganos societarios o de una fundación).

La modificación de los datos del anexo I podrá hacerse por medio de escrito dirigido a la Plataforma de Contratación por el titular de los órganos de contratación unipersonales, o por el Presidente en el caso de órganos de contratación de carácter colegiado, o a través del Portal, en la forma señalada en el apartado séptimo.

Artículo 4. *Sistemas para la interacción con la Plataforma de Contratación del Estado.*

La interacción del órgano de contratación con la Plataforma de Contratación del Estado, a efectos de la publicación de la información relativa a licitaciones, podrá efectuarse a través del Portal o a través de los Servicios web definidos al efecto y publicados en la propia Plataforma, en la forma prevista en los artículos sexto y séptimo.

La información contractual de carácter general, no vinculada a procedimientos concretos de adjudicación, se enviará a la Plataforma a través del Portal, por correo electrónico o por medio de escrito.

Artículo 5. *Servicios prestados por la Plataforma de Contratación del Estado.*

1. Servicios generales. La Plataforma de Contratación del Estado prestará, con carácter general, los siguientes servicios:

a) Publicación de información contractual:

1.1 Relativa a licitaciones concretas y acuerdos marco:

1.1.1 Anuncios:

1.1.1.1 Licitación.
1.1.1.2 Adjudicación provisional.
1.1.1.3 Adjudicación definitiva.
1.1.1.4 Contrataciones programadas: anuncio indicativo previo y otras.

1.1.2 Otra información contractual:

1.1.2.1 Pliegos.
1.1.2.2 Anulación del procedimiento.
1.1.2.3 Consultas formuladas y respuestas aportadas por el órgano de contratación.

1.2 No vinculada a una licitación:

1.2.1 Celebración de acuerdos marco.
1.2.2 Instrucciones internas de contratación.
1.2.3 Modelos de Pliegos particulares para categorías de contratos de naturaleza análoga.

b) Envío de anuncios a diarios oficiales:

BOE. Se efectuará mediante los servicios Web definidos en el documento de especificación de integración de servicios descrito en el anexo IV (el pago del anuncio deberá gestionarse por el órgano de contratación).

DOUE.

c) Servicios de notificación a candidatos o licitadores:

1. Admisión y rechazo de candidatos y los licitadores.
2. Adjudicación provisional.
3. Adjudicación definitiva.
4. Renuncia del órgano de contratación a celebrar un contrato ya convocado.
5. Desistimiento del procedimiento.

d) Sellado de tiempo a través de la FNMT de todos los documentos publicados en la Plataforma, para garantizar de manera fehaciente el momento de inicio de la difusión pública de la información.

2. Sistema para las comunicaciones relativas a las licitaciones. En la interacción con la Plataforma de Contratación del Estado a través del Portal el órgano de contratación podrá utilizar el sistema de generación de anuncios, comunicaciones y notificaciones en los procesos de publicaciones de las licitaciones.

Artículo 6. *Interacción a través de Servicios Web.*

En la interacción con la Plataforma de Contratación del Estado mediante Servicios web, el órgano de contratación comunica en modo sistema a sistema la información que deba ser publicada en la Plataforma en formato CODICE, sistema basado en la transmisión de mensajes según estándar XML.

Tanto los Servicios web como todos los elementos que constituyen CODICE (plantillas, listas genéricas de código, esquemas, etc.) serán publicados y actualizados en el propio Portal.

La comunicación con la Plataforma de Contratación del Estado se realizará de forma segura mediante el uso de certificados electrónicos, según lo estipulado en el anexo IV.

Artículo 7. *Interacción a través del Portal.*

1. Usuarios del órgano de contratación. La interacción del órgano de contratación con la Plataforma de Contratación del Estado a través del Portal se efectuará por los siguientes usuarios, que tendrán las funciones que se señalan en este artículo:

Responsable del órgano de contratación, que será el titular de los órganos de contratación unipersonales o el Presidente de los órganos de contratación de carácter colegiado. El Responsable podrá realizar todas las funciones contempladas en este apartado relativas a la gestión de usuarios (altas y bajas), gestión de espacios de licitación (creación, asignación y reasignación) y gestión de la información contractual (edición y publicación), así como la modificación de los datos correspondientes al perfil del contratante.

Administrador del órgano de contratación, que podrá realizar las funciones correspondientes a la gestión de usuarios (altas y bajas) en relación con los Publicadores y Editores y la asignación y reasignación de espacios de licitación.

Publicador, que podrá realizar funciones de gestión de espacios de licitación (creación, asignación y reasignación en relación con Editores) y de gestión de la información contractual (edición y publicación).

Editor, podrá realizar funciones de edición de la información contractual, preparando la correspondiente documentación, pero sin capacidad para publicarla.

El acceso a la Plataforma por parte de estos usuarios se efectuará usando los correspondientes identificador de usuario y palabra de paso, o un certificado digital de los que se acuerde la admisión general en el ámbito de la Administración General del Estado, de acuerdo con lo establecido en los artículos 17 a 20 de la Ley 11/2007.

2. Alta y baja de Usuarios. El alta del Responsable se efectuará por la Subdirección General de Coordinación de la Contratación Electrónica. A estos efectos, cuando el órgano de contratación pretenda interactuar con la Plataforma de Contratación del Estado a través del Portal, junto con la solicitud de alta y el formulario del anexo I, deberá también remitirse el formulario del anexo II con los datos del Responsable. La Subdirección General de Coordinación de la Contratación Electrónica confirmará el alta del Responsable y le remitirá las correspondientes credenciales para acceso a la Plataforma.

El alta y la baja del Administrador deberán efectuarse por el Responsable del órgano de contratación por escrito dirigido a la Subdirección General de Coordinación de la Contratación Electrónica. Al escrito de alta deberá acompañarse el formulario recogido en el anexo II debidamente cumplimentado. La Subdirección General de Coordinación de la Contratación Electrónica confirmará el alta del Administrador y le remitirá las correspondientes credenciales para acceso a la Plataforma.

El alta y la baja de Publicador/es y Editor/es podrá realizarse por el Responsable o por el Administrador del órgano de contratación, accediendo electrónicamente al Portal y cumplimentando los correspondientes formularios.

Para que pueda procederse a la baja de usuarios que tengan asignadas licitaciones abiertas, deberá seguirse previamente el proceso de reasignación de espacios de licitación y proceder a su atribución a otro usuario.

3. Gestión de la información contractual relativa a licitaciones concretas. La gestión de la información contractual se efectuará a través de los espacios de trabajo donde el órgano de contratación introduce y gestiona los datos necesarios para generar los anuncios, comunicaciones y notificaciones que se deben producir durante los procesos de licitación

La creación de los espacios de trabajo a efectos de generar y publicar anuncios indicativos previos o los anuncios, comunicaciones y notificaciones necesarios para la tramitación de licitaciones concretas podrá ser efectuada por el Responsable o por los Publicadores. Su asignación o reasignación podrán realizarse por el Responsable, en relación con los Publicadores y Editores, y por los Publicadores con respecto a los Editores. El Administrador podrá también proceder a la reasignación de espacios virtuales.

Artículo 8. *Baja del perfil de contratante.*

La baja voluntaria del perfil de contratante, en los casos en que el órgano de contratación no tenga obligación de publicarlo en la Plataforma de Contratación del Estado, deberá solicitarse por el responsable del órgano de contratación, por medio de escrito dirigido a la Subdirección General de Coordinación de la Contratación Electrónica.

En caso de revocación de poderes o delegaciones de competencias que priven de competencia para contratar a un órgano de contratación, la baja deberá solicitarse, por escrito, por el órgano que efectúe tal revocación.

Artículo 9. *Reorganización de unidades.*

En caso de supresión de órganos, la baja del perfil de contratante del órgano suprimido se efectuará en virtud de comunicación cursada por el órgano que asuma las funciones de éste, procediéndose a la oportuna adscripción al sucesor de los espacios de licitación que se refieran a procedimientos de adjudicación en curso.

CAPÍTULO III

Publicación de información por órganos con competencias consultivas o de ordenación en materia de contratación pública

Artículo 10. *Interacción con la Plataforma a efectos de publicar otra información contractual.*

La información relevante que deba publicarse en la Plataforma de Contratación del Estado por la Junta Consultiva de Contratación Administrativa del Estado y organismos similares de las Comunidades Autónomas, así como por los órganos con competencias en materia de ordenación de la contratación pública, será remitida a la Subdirección General de Coordinación de la Contratación Electrónica para su publicación en la Plataforma.

Disposición final única. *Entrada en vigor.*

La presente Orden entrará en vigor el día 2 de mayo de 2008.

ANEXO I

Datos para el alta del perfil del contratante

Tipo de Administración: Tipo de Administración a la que pertenece el Perfil del Contratante (AGE, CC.AA., Entidad Local, etc.)

Nombre del Departamento u órgano de dependencia: Deberá especificarse el nombre del Departamento si existe dependencia (Ministerio, Secretaria de Estado, Organismo Autónomo, etc.)

Nombre del órgano de contratación: Nombre del órgano de contratación al que se le asocia el Perfil del Contratante

Rol del órgano de contratación: Se especificará el rol con el que actúa el órgano de contratación (Central de Compras, Junta de Contratación, órgano de contratación)

CIF: Numero de Identificación Fiscal que utilizará el órgano de contratación

Idioma preferente: Idioma preferente que utilizará el órgano de contratación.

URL del órgano de contratación: URL del Site del órgano de contratación como fuente de información adicional.

Actividad del órgano de contratación: Tipo de actividad del poder adjudicador (Defensa, Economía y Hacienda, Sanidad, Interior, Vivienda, Ocio, Educación, etc.). El campo admite mas de un valor.

Dirección Postal del órgano de contratación:

Nombre de la Calle.
Código Postal.
Población.
País.
Contacto del Perfil del Contratante.
Teléfono.
Fax.
Email: Dirección de correo Electrónica de la persona de contacto del órgano de contratación.

Integración con la Plataforma:

URL de Recepción de Ofertas: Dirección única que identificará el Servicio Web donde el órgano de contratación desea recibir las Ofertas recibidas a través de la Plataforma en las licitaciones electrónicas. Esta dirección será necesaria solo para aquellos casos en que el órgano de contratación posea un sistema informático propio que le permita efectuar procesos de licitación electrónica.
Tipo de Integración: Modo en el que el órgano de contratación puede integrarse con la Plataforma (Portal o Sistémica).
Certificado del órgano de contratación: En el caso de que el Tipo de integración sea sistémica, el órgano de contratación adjuntará, con la petición de alta, un fichero en Base64 con la parte pública del Certificado de componente emitido por una Autoridad de Certificación reconocida en la Administración General del Estado.

ANEXO II

Alta de un usuario

Nombre:
Apellidos:
Documento de Identificación (DNI/NIE):
Rol: Funciones que desempeñará el usuario del que se solicita el alta dentro de la Plataforma.

Según la definición de roles en la Plataforma, este campo podrá tener los siguientes valores:

ROC (responsable del órgano de contratación).
AOC (Administrador del órgano de contratación).
POC-PUB (Publicador del órgano de contratación).
POC-ED (Editor del órgano de contratación).

Cargo: Cargo que desempeña el usuario dentro del órgano de contratación.
Email: Dirección de correo Electrónica del usuario para el que se solicita el Alta.

ANEXO III

Especificaciones de contenidos y formatos correspondientes a la arquitectura de información CODICE

CODICE es una librería de componentes y documentos electrónicos estándar para el desarrollo de aplicaciones de contratación pública electrónica de conformidad con los procedimientos y prescripciones de la Directiva 2004/18 y de la Ley 30/2007, de 30 de octubre de 2007, de Contratos del Sector Público, así como con los estándares y

recomendaciones internacionales aplicables a la identificación, denominación, definición y construcción de dichos componentes.

La arquitectura desarrollada proporciona la biblioteca de componentes estándar, reutilizables, y extensibles o adaptables a diversos contextos o necesidades de contratos públicos específicos, para satisfacer las necesidades de información de los documentos y mensajes intercambiados a lo largo del ciclo completo de los procedimientos electrónicos de contratación contemplados en la citada Directiva.

Dichos componentes deberían ser además suficientes para la construcción a partir de ellos de cualquier documento o mensaje estructurado (o estructurable) intercambiado entre los participantes de un proceso de contratación pública susceptible de conversión a formato electrónico funcionalmente equivalente.

CODICE proporciona una biblioteca con los documentos electrónicos estandarizados básicos o comunes utilizados en dichos procedimientos, construidos a partir de la librería de los componentes.

La última versión de la especificación técnica de los documentos electrónicos CODICE se puede encontrar en el Portal de la Plataforma de Contratación del Estado http://contrataciondelestado.es y contempla los siguientes documentos:

1. Anuncio de licitación (ContractNotice): Documento que utiliza un órgano de contratación para anunciar el proyecto de adquisición de bienes, servicios u obras. El anuncio de licitación se publicará en el perfil del contratante y si se supera el umbral legal deberá ser publicado en otras publicaciones como el Diario Oficial de la Unión Europea.

2. Anuncio Previo (PriorInformationNotice): Documento que utiliza un órgano de contratación para declarar la intención de comprar bienes, servicios o trabajos durante un período de tiempo determinado. Se trata de un documento no vinculante que puede ser usado para declarar la voluntad de adquirir durante un período, y tiene el efecto de permitir que el órgano de contratación pueda reducir los plazos en el proceso de licitación.

3. Anuncio de Adjudicación (ContractAwardNotice): Documento publicado por un órgano de contratación para anunciar la adjudicación de un contrato.

4. Pliegos (ContractDocuments): Documento que un órgano de contratación publica o envía a un empresario para ofrecerle información acerca de un contrato en licitación. Este es el principal documento para la licitación, en él, los órganos de contratación especifican el objeto del contrato, el proceso de licitación y sus condiciones.

5. Oferta (Tender): Documento mediante el cual un licitador ofrece sus productos, servicios o proyectos como respuesta a una licitación.

6. Declaración (Declaration): Documento que utiliza el operador económico para realizar declaraciones sobre su propia condición. Se utiliza para permitir al órgano de contratación evaluar la capacidad del operador económico de participar en el proceso de licitación.

7. Garantía (Guarantee): Documento para notificar el depósito de una garantía.

8. Notificación de adjudicación (AwardNotification): Documento que se utiliza para comunicar la adjudicación del contrato al adjudicatario.

9. Notificación de no adjudicación (UnawardedNotification): Documento que se utiliza para comunicar la adjudicación del contrato a otro licitador.

10. Notificación de admisión/exclusión (QualificationResultNotification): Documento que el órgano de contratación envía a un operador económico a fin de notificarle su admisión o exclusión al proceso de licitación.

11. Notificación de recurso (AppealNotification): Documento que el órgano de contratación envía a todos los licitadores en un proceso de licitación ante la eventual presentación de un recurso por parte de uno de los licitadores.

12. Notificación de recepción de oferta (TenderReceptionNotification): Documento enviado por el órgano de contratación a un operador económico para notificar de la recepción de la oferta de licitación. Está firmado por el órgano de contratación para que el licitador obtenga una prueba de presentación.

13. Invitación a licitar (InvitationToTender): Documento enviado por el órgano de contratación a un operador económico invitándolo a presentar oferta a un proceso de licitación.

14. Solicitud de pliegos (ContractDocumentsRequest): Documento enviado por el operador económico solicitando la documentación del contrato. En algunos procesos de

licitación, los pliegos no son de acceso público, por lo que los licitadores deben solicitarlo mediante este documento

15. Solicitud de subsanación (ClarifyingRequest): Documento enviado por el órgano de contratación a un operador económico solicitando aclaraciones o nueva documentación para poder evaluarle como candidato válido para un proceso de licitación.

Toda la documentación completa necesaria para la implementación de CODICE, así como las modificaciones que pudiera producirse, de uso libre y gratuito, estará a disposición pública en el Portal de la Plataforma de Contratación del Estado (http://contrataciondelestado.es), con el contenido que se detalla a continuación:

1. Memoria CODICE:

Análisis de procedimientos de contratación: estudio de los distintos procedimientos de contratación previstos en la Directiva Europea 2004/18/CE y en la Ley de Contratos del Sector Público española

Normalización UMM de procesos de negocio: representación de los procesos de negocio y de las transacciones implicadas en la contratación electrónica.

2. Mapa ontológico: Contiene todos los componentes CODICE, más los reutilizados de UBL en un único diagrama de clases. Ensamblando estos componentes se han construido los documentos CODICE. Estos mismos componentes podrán utilizarse para crear nuevos documentos.

3. Documentos ensamblados: creados a partir de componentes, con varias representaciones de dichos documentos:

Diagramas de clases. Modelos UML de los documentos CODICE.

Modelo de datos en hoja de calculo.

Esquemas XSD v1.04. Contiene la definición de la estructura XML que deben cumplir los documentos CODICE. Se utilizan para validar los documentos CODICE.

XML de ejemplo.

Guías de implementación. Explicación de cómo implementar cada uno de los documentos CODICE.

4. Listas de códigos: Listas de valores para aquellos elementos de datos que requieren codificación.

ANEXO IV

Especificaciones de los protocolos de comunicación de información

La Plataforma de Contratación del Estado, en cumplimiento de la normativa aplicable, facilita una serie de servicios de publicación para los Órganos de Contratación de la Administración mediante un acceso Web al Portal de Contratación y mediante acceso sistémico de maquina a maquina denominado integración B2B.

Los servicios expuestos por la plataforma para la publicación sistema a sistema son los relativos a los siguientes casos de uso:

1. Solicitud de publicación de anuncios y pliegos:

a) Publicación del Anuncio Previo
b) Publicación del Anuncio del Licitación
c) Publicación del Documento de Pliego
d) Publicación del Anuncio de Adjudicación

2. Solicitud de estado de un Espacio Virtual de Licitación (EVL). El EVL es un concepto que maneja la Plataforma y que se equipara al conjunto de datos del expediente (interno al órgano de contratación) al que hay que dar publicidad.

3. Reenvío de las Ofertas recibidas en la Plataforma de contratación a los sistemas de los Órganos de Contratación.

Como mecanismo de comunicación sistema a sistema entre la Plataforma de Contratación del Estado y los Órganos de Contratación se utiliza tecnología Web Services con las siguientes características:

Uso de mensajería SOAP sobre un transporte síncrono petición/respuesta como http(s).

Definición de servicios mediante el lenguaje de definición de servicios Web WSDL.

Uso de canal cifrado mediante SSL/TLS (https) para preservar la confidencialidad de la información antes de su publicación.

La autenticación de los Órganos de Contratación en la plataforma se realizará mediante la utilización de WebService Security (WS-S). El órgano de contratación firmará las peticiones mediante un Certificado Digital de una Autorizada de Certificación (CA) reconocida, del cual debe facilitarse a la plataforma su parte pública (según se especifica en el anexo I).

La última versión de la especificación técnica de los protocolos de comunicación para el intercambio de contenidos sistema a sistema se puede encontrar en Portal de la Plataforma de Contratación del Estado http://contrataciondelestado.es y consta de los siguientes documentos:

1. Documento de Especificación de Integración de Servicios sistema a sistema (B2B).

2. Documento de Especificación de Reenvío de Oferta mediante mecanismos sistema a sistema (B2B).

Cualquier otro documento que deba utilizarse en nuevas implementaciones, o las modificaciones que puedan producirse en los existentes, será puesto a disposición de los interesados en el portal de la Plataforma de Contratación del estado en la dirección http://contrataciondelestado.es

§ 47

Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público

Jefatura del Estado
«BOE» núm. 311, de 28 de diciembre de 2013
Última modificación: 13 de junio de 2015
Referencia: BOE-A-2013-13722

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley:

PREÁMBULO

Uno de los elementos clave para mejorar la competitividad de las empresas consiste en reducir la morosidad de las Administraciones Públicas, ya que esto permitirá reducir sus necesidades de financiación y evitar los efectos negativos que ello genera sobre el empleo y su propia supervivencia.

Con este objetivo el informe de la Comisión para la reforma de las Administraciones Públicas contiene varias propuestas de reformas estructurales para erradicar la morosidad de las Administraciones Públicas. Esta Ley es una de estas reformas estructurales que impulsa el uso de la factura electrónica y crea el registro contable, lo que permitirá agilizar los procedimientos de pago al proveedor y dar certeza de las facturas pendientes de pago existentes.

Este control informatizado y sistematizado de las facturas favorecerá un seguimiento riguroso de la morosidad a través de un indicador, el periodo medio de pagos, que visualizará el volumen de deuda comercial de las Administraciones y permitirá, llegado el caso, aplicar los nuevos mecanismos previstos la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, en la que el control de la deuda comercial forma parte del principio de sostenibilidad financiera.

Para fortalecer esta necesaria protección del proveedor se facilita su relación con las Administraciones Públicas favoreciendo el uso de la factura electrónica y su gestión y tramitación telemática, en línea con la «Agenda Digital para Europa», una de las iniciativas que la Comisión Europea está impulsando en el marco de la estrategia «Europa 2020». Asimismo, esta protección se verá reforzada con un mejor control contable de las facturas recibidas por las Administraciones, lo cual permitirá no sólo hacer un mejor seguimiento del cumplimiento de los compromisos de pago de las Administraciones Públicas, sino también,

un mejor control del gasto público y del déficit, lo que generará una mayor confianza en las cuentas públicas.

Para alcanzar estos fines, esta Ley incluye medidas dirigidas a mejorar la protección de los proveedores, tales como el establecimiento de la obligación de presentación en un registro administrativo de las facturas expedidas por los servicios que presten o bienes que entreguen a una Administración Pública en el marco de cualquier relación jurídica; el impulso del uso de la factura electrónica en el sector público, con carácter obligatorio para determinados sujetos a partir del quince de enero de 2015; la creación obligatoria para cada una de las Administraciones Públicas, estatal, autonómica y local, de puntos generales de entrada de facturas electrónicas para que los proveedores puedan presentarlas y lleguen electrónicamente al órgano administrativo al que corresponda su tramitación y a la oficina contable competente. De este modo habría un punto general de entrada de facturas electrónicas por cada nivel administrativo, en total tres, salvo que las Comunidades Autónomas o las Entidades Locales, en aplicación del principio de eficiencia, se adhieran al punto general de entrada de facturas electrónicas de la Administración General del Estado.

Por último, se apuesta además por el impulso de la facturación electrónica también en el sector privado, a través de la modificación de la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información, exigible a partir del quince de enero de 2015.

Junto a las medidas adoptadas para proteger al proveedor y con el objetivo de seguir avanzando en un mejor control del gasto público, la presente Ley pone en marcha también unas medidas dirigidas a las Administraciones Públicas como la creación de un registro contable de facturas gestionado por el órgano o unidad que tenga atribuida la función contable; la regulación de un nuevo procedimiento de tramitación de facturas, que entrará en vigor a partir del 1 de enero de 2014, que mejorará el seguimiento de las mismas, y el fortalecimiento de los órganos de control interno al otorgarles la facultad de poder acceder a la documentación contable en cualquier momento.

La presente Ley consta de un total de 13 artículos, agrupados en cinco capítulos, seis disposiciones adicionales, tres disposiciones transitorias, una disposición derogatoria única y ocho disposiciones finales.

El Capítulo I concreta el objeto de la Ley y su ámbito de aplicación subjetivo. La Ley se aplica a las facturas emitidas por la entrega de bienes o la prestación de servicios a las Administraciones Públicas, entendiendo por tales los entes, organismos y entidades a que se refiere el artículo 3.2 del Texto Refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre.

El Capítulo II establece la obligación de presentación de las facturas en un registro administrativo.

El Capítulo III se refiere al uso de la factura electrónica en el sector público, estableciendo el formato que debe tener. Asimismo, se crea el denominado punto general de entrada de facturas electrónicas, del que dispondrán cada una de las Administraciones, con posibilidad de celebrar convenios o adherirse al punto ya implementado por la Administración General del Estado para compartir su uso y que no sea necesario que cada Administración invierta recursos en desarrollar su propio Punto general de entrada de facturas electrónicas. A estos efectos se regulan las características mínimas que deben reunir estos puntos.

El Capítulo IV regula la creación del registro contable de facturas, un nuevo procedimiento para la tramitación de facturas y las actuaciones correspondientes al órgano competente en materia de contabilidad.

El Capítulo V recoge los efectos de la recepción de la factura, las facultades y obligaciones de los órganos de control interno y la colaboración con la Agencia Estatal de Administración Tributaria.

Las disposiciones adicionales primera, segunda, tercera, cuarta, quinta y sexta regulan respectivamente el régimen, a los efectos de esta Ley, de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos, el formato de la factura y la firma electrónica, el formato de la factura electrónica y sus efectos tributarios, el intercambio de información sobre deudores de las Administraciones, la adhesión al punto general de entrada de facturas electrónicas de la Administración General del Estado y la publicidad de

la creación de los puntos generales de entrada de facturas electrónicas y el registro contable de facturas.

La disposición transitoria primera prevé la no aplicación de lo dispuesto en la Ley a las facturas ya expedidas en el momento de su entrada en vigor. No obstante, los proveedores que así lo consideren podrán presentar ante un registro administrativo también las facturas expedidas antes de la entrada en vigor de la Ley.

La disposiciones transitorias segunda y tercera prevén la firma de las facturas electrónicas en tanto no se desarrolle el contenido del sello electrónico avanzado y la intermediación entre el punto general de entrada de facturas y los órganos administrativos a los que corresponda la tramitación, hasta que no estén disponibles los registros contables de facturas respectivamente.

La disposición derogatoria deroga cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la Ley.

La disposición final primera se refiere a la modificación de la Ley 29/1987, de 18 de diciembre, del Impuesto sobre Sucesiones y Donaciones.

La disposición final segunda recoge la modificación de la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información para establecer la obligatoriedad de la facturación electrónica a determinadas empresas y particulares que acepten recibirlas o que las hayan solicitado expresamente, así como la eficacia ejecutiva de la factura electrónica.

La disposición final tercera se refiere a la modificación del texto refundido de la Ley de Contratos del Sector Público.

La disposición final cuarta se refiere a una modificación de la Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización.

La disposición final quinta determina el carácter básico de la Ley e invoca los artículos 149.1.6.ª, 149.1.8.ª, 149.1.13.ª, 149.1.14.ª y 149.1.18.ª de la Constitución española como títulos competenciales al amparo de los cuales se dicta la Ley.

Las disposiciones finales sexta, séptima y octava se refieren respectivamente al desarrollo reglamentario de esta Ley, la habilitación normativa y su entrada en vigor a los veinte días de su publicación en el Boletín Oficial del Estado, salvo el artículo 4, que entrará en vigor el 15 de enero de 2015, y el artículo 9 y la disposición final primera, que entrarán en vigor el 1 de enero de 2014.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

Constituye el objeto de la presente Ley impulsar el uso de la factura electrónica, crear el registro contable de facturas, regular el procedimiento para su tramitación en las Administraciones públicas y las actuaciones de seguimiento por los órganos competentes.

Artículo 2. *Ámbito de aplicación subjetivo.*

1. Lo previsto en la presente Ley será de aplicación a las facturas emitidas en el marco de las relaciones jurídicas entre proveedores de bienes y servicios y las Administraciones Públicas.

2. A los efectos de lo previsto en esta Ley tendrán la consideración de Administraciones Públicas los entes, organismos y entidades a que se refiere el artículo 3.2 del Texto Refundido de la Ley de Contratos del Sector Público, aprobado por Real Decreto Legislativo 3/2011, de 14 de noviembre, así como las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, en el ejercicio de su función colaboradora en la gestión de la Seguridad Social.

CAPÍTULO II

Obligación de presentación de facturas ante las Administraciones Públicas

Artículo 3. *Obligación de presentación de facturas en el registro.*

El proveedor que haya expedido la factura por los servicios prestados o bienes entregados a cualquier Administración Pública, tendrá la obligación, a efectos de lo dispuesto en esta Ley, de presentarla ante un registro administrativo, en los términos previstos en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en el plazo de treinta días desde la fecha de entrega efectiva de las mercancías o la prestación de servicios. En tanto no se cumplan los requisitos de tiempo y forma de presentación establecidos en esta Ley no se entenderá cumplida esta obligación de presentación de facturas en el registro.

CAPÍTULO III

Factura electrónica en las Administraciones Públicas

Artículo 4. *Uso de la factura electrónica en el sector público.*

1. Todos los proveedores que hayan entregado bienes o prestado servicios a la Administración Pública podrán expedir y remitir factura electrónica. En todo caso, estarán obligadas al uso de la factura electrónica y a su presentación a través del punto general de entrada que corresponda, las entidades siguientes:

a) Sociedades anónimas;
b) Sociedades de responsabilidad limitada;
c) Personas jurídicas y entidades sin personalidad jurídica que carezcan de nacionalidad española;
d) Establecimientos permanentes y sucursales de entidades no residentes en territorio español en los términos que establece la normativa tributaria;
e) Uniones temporales de empresas;
f) Agrupación de interés económico, Agrupación de interés económico europea, Fondo de Pensiones, Fondo de capital riesgo, Fondo de inversiones, Fondo de utilización de activos, Fondo de regularización del mercado hipotecario, Fondo de titulización hipotecaria o Fondo de garantía de inversiones.

No obstante, las Administraciones Públicas podrán excluir reglamentariamente de esta obligación de facturación electrónica a las facturas cuyo importe sea de hasta 5.000 euros y a las emitidas por los proveedores a los servicios en el exterior de las Administraciones Públicas hasta que dichas facturas puedan satisfacer los requerimientos para su presentación a través del Punto general de entrada de facturas electrónicas, de acuerdo con la valoración del Ministerio de Hacienda y Administraciones Públicas, y los servicios en el exterior dispongan de los medios y sistemas apropiados para su recepción en dichos servicios.

2. Todos los proveedores tienen derecho a ser informados sobre el uso de la factura electrónica a través del órgano, organismo público o entidad que determine cada Administración Pública.

Artículo 5. *Formato de las facturas electrónicas y su firma electrónica.*

A efectos de lo previsto en esta Ley:

1. Las facturas electrónicas que se remitan a las Administraciones Públicas deberán tener un formato estructurado y estar firmadas con firma electrónica avanzada basada en un certificado reconocido, de acuerdo con lo dispuesto en el artículo 10.1 a) del Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación.

Por Orden de la Vicepresidenta del Gobierno y Ministra de la Presidencia, a propuesta conjunta del Ministro de Hacienda y Administraciones Públicas y del Ministro de Industria, Energía y Turismo, se determinará el formato estructurado de la factura electrónica, oído el comité sectorial de Administración electrónica.

2. También se admitirá el sello electrónico avanzado basado en un certificado reconocido que reúna los siguientes requisitos:

a) El certificado deberá identificar a la persona jurídica o entidad sin personalidad jurídica que selle la factura electrónica, a través de su denominación o razón social y su número de identificación fiscal.

b) La solicitud del sello electrónico avanzado podrá formularse bien mediante comparecencia presencial de una persona física que acredite su representación, bien por medios electrónicos mediante el DNI electrónico y la remisión de los documentos que acrediten su poder de representación en formato papel o electrónico.

El sello electrónico es el conjunto de datos en forma electrónica, consignados o asociados con facturas electrónicas, que pueden ser utilizados por personas jurídicas y entidades sin personalidad jurídica para garantizar el origen y la integridad de su contenido.

Artículo 6. *Punto general de entrada de facturas electrónicas.*

1. El Estado, las Comunidades Autónomas y las Entidades locales, dispondrán de un Punto general de entrada de facturas electrónicas, a través del cual se recibirán todas las facturas electrónicas que correspondan a entidades, entes y organismos vinculados o dependientes.

No obstante lo anterior, las Entidades Locales podrán adherirse a la utilización del Punto general de entrada de facturas electrónicas que proporcione su Diputación, Comunidad Autónoma o el Estado.

Asimismo, las Comunidades Autónomas podrán adherirse a la utilización del Punto general de entrada de facturas electrónicas que proporcione el Estado.

2. El Punto general de entrada de facturas electrónicas de una Administración proporcionará una solución de intermediación entre quien presenta la factura y la oficina contable competente para su registro.

3. El Punto general de entrada de facturas electrónicas permitirá el envío de facturas electrónicas en el formato que se determina en esta Ley. El proveedor o quien haya presentado la factura podrá consultar el estado de la tramitación de la factura.

4. Todas las facturas electrónicas que reúnan los requisitos previstos en esta Ley y su normativa básica de desarrollo, sin perjuicio de ulteriores requisitos que en la fase de conformidad deban cumplirse, serán presentadas a través del Punto general de entrada de facturas electrónicas, donde serán admitidas, y producirán una entrada automática en un registro electrónico de la Administración Pública gestora de dicho Punto general de entrada de facturas electrónicas, proporcionando un acuse de recibo electrónico con acreditación de la fecha y hora de presentación.

5. El Punto general de entrada de facturas electrónicas proporcionará un servicio automático de puesta a disposición o de remisión electrónica de las mismas a las oficinas contables competentes para su registro.

6. La Secretaría de Estado de Administraciones Públicas y la Secretaría de Estado de Presupuestos y Gastos determinarán conjuntamente las condiciones técnicas normalizadas del Punto general de entrada de facturas electrónicas así como los servicios de interoperabilidad entre el resto de Puntos con el Punto general de entrada de facturas electrónicas de la Administración General del Estado.

7. Cuando una Administración Pública no disponga de Punto general de entrada de facturas electrónicas ni se haya adherido al de otra Administración, el proveedor tendrá derecho a presentar su factura en el Punto general de entrada de facturas electrónicas de la Administración General del Estado, quien depositará automáticamente la factura en un repositorio donde la Administración competente será responsable de su acceso, y de la gestión y tramitación de la factura.

8. Las diputaciones provinciales, cabildos y consejos insulares ofrecerán a los municipios con población inferior a 20.000 habitantes la colaboración y los medios técnicos necesarios

para posibilitar la aplicación de lo dispuesto en este artículo, de acuerdo con lo establecido en el artículo 36.1 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

Artículo 7. *Archivo y custodia de la información.*

1. La responsabilidad del archivo y custodia de las facturas electrónicas corresponde al órgano administrativo destinatario de la misma, sin perjuicio de que pueda optar por la utilización del correspondiente punto general de entrada de facturas electrónicas como medio de archivo y custodia de dichas facturas si se adhiere al mismo.

2. Cuando el punto general de entrada de facturas electrónicas sea utilizado para archivo y custodia de las facturas electrónicas, su información no podrá ser empleada para la explotación o cesión de la información, salvo para el propio órgano administrativo al que corresponda la factura. Ello se entenderá sin perjuicio de las obligaciones que se puedan derivar de la normativa tributaria.

CAPÍTULO IV

Registro contable de facturas y procedimiento de tramitación en las Administraciones Públicas

Artículo 8. *Creación del registro contable de facturas.*

1. Cada uno de los sujetos incluidos en el ámbito de aplicación de esta Ley, dispondrán de un registro contable de facturas que facilite su seguimiento, cuya gestión corresponderá al órgano o unidad administrativa que tenga atribuida la función de contabilidad.

2. Dicho registro contable de facturas estará interrelacionado o integrado con el sistema de información contable.

Artículo 9. *Procedimiento para la tramitación de facturas.*

1. El registro administrativo en el que se reciba la factura la remitirá inmediatamente a la oficina contable competente para la anotación en el registro contable de la factura.

Las facturas electrónicas presentadas en el correspondiente Punto general de entrada de facturas electrónicas, serán puestas a disposición o remitidas electrónicamente, mediante un servicio automático proporcionado por dicho Punto, al registro contable de facturas que corresponda en función de la oficina contable que figura en la factura. En la factura deberán identificarse los órganos administrativos a los que vaya dirigida de conformidad con la disposición adicional trigésima tercera del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre. No obstante, el Estado, las Comunidades Autónomas y los municipios de Madrid y Barcelona, podrán excluir reglamentariamente de esta obligación de anotación en el registro contable a las facturas en papel cuyo importe sea de hasta 5.000 euros, así como las facturas emitidas por los proveedores a los servicios en el exterior de cualquier Administración Pública hasta que dichas facturas puedan satisfacer los requerimientos para su presentación a través del Punto general de entrada de facturas electrónicas, de acuerdo con la valoración del Ministerio de Hacienda y Administraciones Públicas, y los servicios en el exterior dispongan de los medios y sistemas apropiados para su recepción en dichos servicios.

Los registros contables de facturas se podrán conectar con distintos Puntos generales de entrada de facturas electrónicas y en todo caso se conectarán con el Punto general de entrada de facturas electrónicas de la Administración General del Estado cuando la Administración correspondiente se hubiera adherido al uso del mismo.

2. La anotación de la factura en el registro contable de facturas dará lugar a la asignación del correspondiente código de identificación de dicha factura en el citado registro contable. En el caso de las facturas electrónicas dicho código será automáticamente asignado y comunicado inmediatamente a los Puntos generales de entrada de facturas electrónicas con los que esté interconectado el registro contable, pudiendo rechazarse la factura en esta fase solamente cuando no se cumplan los requisitos previstos en esta Ley y su normativa básica de desarrollo.

3. El órgano o unidad administrativa que tenga atribuida la función de contabilidad la remitirá o pondrá a disposición del órgano competente para tramitar, si procede, el procedimiento de conformidad con la entrega del bien o la prestación del servicio realizada por quien expidió la factura y proceder al resto de actuaciones relativas al expediente de reconocimiento de la obligación, incluida, en su caso, la remisión al órgano de control competente a efectos de la preceptiva intervención previa.

4. Una vez reconocida la obligación por el órgano competente que corresponda, la tramitación contable de la propuesta u orden de pago identificará la factura o facturas que son objeto de la propuesta, mediante los correspondientes códigos de identificación asignados en el registro contable de facturas.

Artículo 10. *Actuaciones del órgano competente en materia de contabilidad.*

Los órganos o unidades administrativas que tengan atribuida la función de contabilidad en las Administraciones Públicas:

1. Efectuarán requerimientos periódicos de actuación respecto a las facturas pendientes de reconocimiento de obligación, que serán dirigidos a los órganos competentes.

2. Elaborarán un informe trimestral con la relación de las facturas con respecto a los cuales hayan transcurrido más de tres meses desde que fueron anotadas y no se haya efectuado el reconocimiento de la obligación por los órganos competentes. Este informe será remitido dentro de los quince días siguientes a cada trimestre natural del año al órgano de control interno.

CAPÍTULO V

Efectos de la recepción de la factura, facultades de los órganos de control y colaboración con la Agencia Estatal de Administración Tributaria

Artículo 11. *Efectos de la recepción de la factura en el punto general de entrada de facturas electrónicas y anotación en el registro contable de facturas.*

La recepción de la factura en el punto general de entrada de facturas electrónicas y su anotación en el registro contable de facturas tendrá únicamente los efectos que de acuerdo con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común se deriven de su presentación en un registro administrativo.

Artículo 12. *Facultades y obligaciones de los órganos de control interno.*

1. La Intervención General de la Administración del Estado y los órganos de control equivalentes en los ámbitos autonómico y local tendrán acceso a la documentación justificativa, a la información que conste en el registro contable de facturas, y a la contabilidad en cualquier momento.

2. Anualmente, el órgano de control interno elaborará un informe en el que evaluará el cumplimiento de la normativa en materia de morosidad. En el caso de las Entidades Locales, este informe será elevado al Pleno.

3. Las Intervenciones Generales u órganos equivalentes de cada Administración realizarán una auditoría de sistemas anual para verificar que los correspondientes registros contables de facturas cumplen con las condiciones de funcionamiento previstas en esta Ley y su normativa de desarrollo y, en particular, que no quedan retenidas facturas presentadas en el Punto general de entrada de facturas electrónicas que fueran dirigidas a órganos o entidades de la respectiva Administración en ninguna de las fases del proceso. En este informe se incluirá un análisis de los tiempos medios de inscripción de facturas en el registro contable de facturas y del número y causas de facturas rechazadas en la fase de anotación en el registro contable.

Artículo 13. *Colaboración con la Agencia Estatal de Administración Tributaria.*

Los registros contables de facturas remitirán a la Agencia Estatal de Administración Tributaria, por vía telemática, aquella información sobre las facturas recibidas, para asegurar el cumplimiento de las obligaciones tributarias y de facturación cuyo control le corresponda. Se habilita al Ministro de Hacienda y Administraciones Públicas a determinar el contenido de la información indicada así como el procedimiento y periodicidad de su remisión.

Disposición adicional primera. *Régimen de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos.*

Los órganos competentes del Congreso de los Diputados, del Senado, del Consejo General del Poder Judicial, del Tribunal Constitucional, del Tribunal de Cuentas, del Defensor del Pueblo, de las Asambleas Legislativas de las Comunidades Autónomas y de las instituciones autonómicas análogas al Tribunal de Cuentas y al Defensor del Pueblo adaptarán su actuación a las normas establecidas en esta Ley para las Administraciones Públicas.

Disposición adicional segunda. *Formato de la factura y firma electrónica.*

En tanto no se apruebe la Orden ministerial prevista en el artículo 5, las facturas electrónicas que se remitan a las Administraciones Públicas se ajustarán al formato estructurado de la factura electrónica Facturae, versión 3.2, y de firma electrónica conforme a la especificación XMLAdvanced Electronic Signatures (XAdES).

Disposición adicional tercera. *Formato de la factura electrónica y sus efectos tributarios.*

La factura electrónica prevista en esta Ley y su normativa de desarrollo será válida y tendrá los mismos efectos tributarios que la factura en soporte papel. En particular, podrá ser utilizada como justificante a efectos de permitir la deducibilidad de la operación de conformidad con la normativa de cada tributo y lo dispuesto en el artículo 106 de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional cuarta. *Intercambio de información.*

La Agencia Estatal de Administración Tributaria, los órganos de recaudación de la Comunidades Autónomas y Entidades Locales, la Tesorería General de la Seguridad Social y los órganos pagadores de las Administraciones públicas, incluidas en el ámbito de aplicación de esta Ley, de acuerdo con el procedimiento que se establezca reglamentariamente, intercambiarán la información sobre deudores de las Administraciones y los pagos a los mismos con el objeto de realizar las actuaciones de embargo o compensación que procedan.

La Agencia Estatal de Administración Tributaria creará y administrará la plataforma informática para el desarrollo de los intercambios de información y las actuaciones de gestión recaudatoria previstas en esta disposición.

Disposición adicional quinta. *Adhesión al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado.*

1. En cumplimiento de la obligación de establecer un punto general de entrada de facturas electrónicas señalada en el artículo 6 de la presente Ley, las Comunidades Autónomas y las Entidades Locales podrán adherirse al punto general de entrada de facturas electrónicas establecido por la Administración General del Estado, que les proporcionará las funcionalidades previstas para el citado punto respecto de las facturas electrónicas de los proveedores.

2. La adhesión al punto general de entrada de facturas electrónicas de la Administración General del Estado se realizará por medios telemáticos a través del portal electrónico establecido al efecto en el citado punto por la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas.

3. Este acto de adhesión, suscrito con firma electrónica avanzada por el órgano competente de la Comunidad Autónoma o Entidad Local de que se trate, deberá dejar

constancia de la voluntad de dicha Comunidad o Entidad de adherirse al punto general de entrada de facturas electrónicas de la Administración General del Estado y de aceptar en su integridad las condiciones de uso de la plataforma, determinadas por la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas.

4. Los desarrollos técnicos que, en su caso, deban implantar las Comunidades Autónomas y las Entidades Locales para integrar y hacer compatibles sus sistemas informáticos con el punto general de entrada de facturas electrónicas de la Administración General del Estado serán financiados con cargo a los Presupuestos de cada Comunidad Autónoma o Entidad Local.

5. La adhesión de las Comunidades Autónomas o Entidades Locales al punto general de entrada de facturas electrónicas de la Administración General del Estado es voluntaria, si bien la no adhesión deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

La adhesión al punto general entrada de facturas electrónicas de la Administración General del Estado podrá conllevar la repercusión de los costes económicos que se generen.

Disposición adicional sexta. *Publicidad de los Puntos generales de entrada de facturas electrónicas y de los registros contables.*

1. A la creación de los Puntos generales de entrada de facturas electrónicas y de los registros contables se le dará publicidad.

2. El Ministerio de Hacienda y Administraciones Públicas mantendrá actualizado un Directorio en el que la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales consignarán, al menos, la dirección electrónica de su Punto general de entrada de facturas electrónicas y el resto de información complementaria que pueda ser útil para que sea consultado por los proveedores.

3. Las diputaciones provinciales, cabildos y consejos insulares ofrecerán a los municipios con población inferior a 20.000 habitantes la colaboración y los medios técnicos necesarios para posibilitar la aplicación de lo previsto en esta disposición, de acuerdo con lo establecido en el artículo 36.1 de la Ley 7/1985, de 2 de abril, reguladora de las Bases del Régimen Local.

Disposición transitoria primera. *Obligación de presentación de la factura en un registro administrativo.*

Las obligaciones previstas en esta Ley no serán de aplicación a las facturas ya expedidas en el momento de su entrada en vigor.

No obstante, el proveedor que haya expedido la factura por los servicios prestados o bienes entregados a cualquier Administración Pública antes de la entrada en vigor de esta Ley podrá presentarla ante un registro administrativo, en los términos previstos en el artículo 38 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Disposición transitoria segunda. *Firma de las facturas electrónicas.*

En tanto no se desarrolle el contenido del sello electrónico avanzado basado en un certificado electrónico reconocido, las facturas electrónicas que se presenten ante las Administraciones Públicas podrán garantizar su autenticidad e integridad mediante un certificado que resulte válido en la plataforma de validación de certificados electrónicos @firma del Ministerio de Hacienda y Administraciones Públicas.

Disposición transitoria tercera. *Intermediación entre el punto general de entrada de facturas y la oficina contable competente.*

Mientras no esté disponible el registro contable de facturas, el punto general de entrada de facturas electrónicas proporcionará una solución de intermediación, bien a través de un servicio automático de puesta a disposición o bien a través de su remisión electrónica, entre quien presenta la factura y el órgano administrativo al que corresponda su tramitación.

Disposición derogatoria. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en la presente Ley. En particular, queda derogado el artículo 5 de la Ley 15/2010, de 5 de julio, de modificación de la Ley 3/2004, de 29 de diciembre, por la que se establecen medidas de lucha contra la morosidad en las operaciones comerciales.

Disposición final primera. *Modificación de la Ley 29/1987, de 18 de diciembre, del Impuesto sobre Sucesiones y Donaciones.*

Se modifica el apartado 4 del artículo 34 de la Ley 29/1987, de 18 de diciembre, del Impuesto sobre Sucesiones y Donaciones, que queda redactado de la siguiente forma:

«4. De acuerdo con lo dispuesto en el apartado anterior, se establece el régimen de autoliquidación del impuesto con carácter obligatorio en las siguientes Comunidades Autónomas:

Comunidad Autónoma de Andalucía
Comunidad Autónoma de Aragón
Comunidad Autónoma del Principado de Asturias
Comunidad Autónoma de las Illes Balears
Comunidad Autónoma de Canarias
Comunidad Autónoma de Castilla-La Mancha
Comunidad de Castilla y León
Comunidad Autónoma de Cataluña
Comunidad Autónoma de Galicia
Comunidad Autónoma de la Región de Murcia
Comunidad Valenciana»

Disposición final segunda. *Modificación de la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información.*

La Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información, queda modificada como sigue:

Uno. Se incluye un nuevo artículo 2 bis con la siguiente redacción:

«Artículo 2 bis. *Factura electrónica en el sector privado.*

A efectos de lo dispuesto en esta Ley:

1. Las empresas prestadoras de los servicios a que alude el artículo 2.2, deberán expedir y remitir facturas electrónicas en sus relaciones con empresas y particulares que acepten recibirlas o que las hayan solicitado expresamente. Este deber es independiente del tamaño de su plantilla o de su volumen anual de operaciones.

No obstante, las agencias de viaje, los servicios de transporte y las actividades de comercio al por menor sólo están obligadas a emitir facturas electrónicas en los términos previstos en el párrafo anterior cuando la contratación se haya llevado a cabo por medios electrónicos.

Las obligaciones previstas en este artículo no serán exigibles hasta el 15 de enero de 2015.

2. El Gobierno podrá ampliar el ámbito de aplicación de este artículo a empresas o entidades que no presten al público en general servicios de especial trascendencia económica en los casos en que se considere que deban tener una interlocución telemática con sus clientes o usuarios, por la naturaleza de los servicios que prestan, y emitan un número elevado de facturas.

3. Las facturas electrónicas deberán cumplir, en todo caso, lo dispuesto en la normativa específica sobre facturación.

4. Las empresas prestadoras de servicios deberán facilitar acceso a los programas necesarios para que los usuarios puedan leer, copiar, descargar e imprimir la factura electrónica de forma gratuita sin tener que acudir a otras fuentes para proveerse de las aplicaciones necesarias para ello.

Deberán habilitar procedimientos sencillos y gratuitos para que los usuarios puedan revocar el consentimiento dado a la recepción de facturas electrónicas en cualquier momento.

5. El período durante el que el cliente puede consultar sus facturas por medios electrónicos establecido en el artículo 2.1 b) no se altera porque aquel haya resuelto su contrato con la empresa o revocado su consentimiento para recibir facturas electrónicas. Tampoco caduca por esta causa su derecho a acceder a las facturas emitidas con anterioridad.

6. Las empresas que, estando obligadas a ello, no ofrezcan a los usuarios la posibilidad de recibir facturas electrónicas o no permitan el acceso de las personas que han dejado de ser clientes, a sus facturas, serán sancionadas con apercibimiento o una multa de hasta 10.000 euros. La sanción se determinará y graduará conforme a los criterios establecidos en el artículo 33 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Idéntica sanción puede imponerse a las empresas que presten servicios al público en general de especial trascendencia económica que no cumplan las demás obligaciones previstas en el artículo 2.1.

Es competente para imponer esta sanción el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.»

Dos. Se incluye un nuevo artículo 2 ter con la siguiente redacción:

«Artículo 2 ter. *Eficacia ejecutiva de la factura electrónica.*

1. La factura electrónica podrá pagarse mediante adeudo domiciliado si se incluye en la correspondiente extensión el identificador de cuenta de pago del deudor y en un anexo, el documento que acredite el consentimiento del deudor a que se refiere la Ley 16/2009, de 13 de noviembre, de servicios de pago.

2. Las facturas electrónicas llevarán aparejada ejecución si las partes así lo acuerdan expresamente. En ese caso, su carácter de título ejecutivo deberá figurar en la factura y el acuerdo firmado entre las partes por el que el deudor acepte dotar de eficacia ejecutiva a cada factura, en un anexo. En dicho acuerdo se hará referencia a la relación subyacente que haya originado la emisión de la factura.

La falta de pago de la factura que reúna estos requisitos, acreditada fehacientemente o, en su caso, mediante la oportuna declaración emitida por la entidad domiciliaria, faculta al acreedor para instar su pago mediante el ejercicio de una acción ejecutiva de las previstas en el artículo 517 de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

3. En las relaciones con consumidores y usuarios, la factura electrónica no podrá tener eficacia ejecutiva.

4. Lo dispuesto en este artículo no será aplicable al pago de las facturas que tengan por destinatarios a los órganos, organismos y entidades integrantes del sector público.»

Disposición final tercera. *Modificación del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre.*

Uno. Se suprime la letra f) del apartado 2 del artículo 3 del texto refundido de la Ley de Contratos del Sector Público.

Dos. Se suprime el apartado 2 del artículo 41 del texto refundido de la Ley de Contratos del Sector Público.

Tres. Se modifica el apartado 1 del artículo 65 del texto refundido de la Ley de Contratos del Sector Público, que queda redactado de la siguiente manera:

«Artículo 65. *Exigencia y efectos de la clasificación.*

1. La clasificación de los empresarios como contratistas de obras o como contratistas de servicios de las Administraciones Públicas será exigible y surtirá efectos para la acreditación de su solvencia para contratar en los siguientes casos y términos:

a) Para los contratos de obras cuyo valor estimado sea igual o superior a 500.000 euros será requisito indispensable que el empresario se encuentre debidamente clasificado como contratista de obras de las Administraciones Públicas. Para dichos contratos, la clasificación del empresario en el grupo o subgrupo que en función del objeto del contrato corresponda, con categoría igual o superior a la exigida para el contrato, acreditará sus condiciones de solvencia para contratar.

Para los contratos de obras cuyo valor estimado sea inferior a 500.000 euros la clasificación del empresario en el grupo o subgrupo que en función del objeto del contrato corresponda acreditará su solvencia económica y financiera y solvencia técnica para contratar. En tales casos, el empresario podrá acreditar su solvencia indistintamente mediante su clasificación como contratista de obras en el grupo o subgrupo de clasificación correspondiente al contrato o bien acreditando el cumplimiento de los requisitos específicos de solvencia exigidos en el anuncio de licitación o en la invitación a participar en el procedimiento y detallados en los pliegos del contrato. En defecto de estos, la acreditación de la solvencia se efectuará con los requisitos y por los medios que reglamentariamente se establezcan en función de la naturaleza, objeto y valor estimado del contrato, medios y requisitos que tendrán carácter supletorio respecto de los que en su caso figuren en los pliegos.

b) Para los contratos de servicios no será exigible la clasificación del empresario. En el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato se establecerán los criterios y requisitos mínimos de solvencia económica y financiera y de solvencia técnica o profesional tanto en los términos establecidos en los artículos 75 y 78 de la Ley como en términos de grupo o subgrupo de clasificación y de categoría mínima exigible, siempre que el objeto del contrato esté incluido en el ámbito de clasificación de alguno de los grupos o subgrupos de clasificación vigentes, atendiendo para ello al código CPV del contrato. En tales casos, el empresario podrá acreditar su solvencia indistintamente mediante su clasificación en el grupo o subgrupo de clasificación correspondiente al contrato o bien acreditando el cumplimiento de los requisitos específicos de solvencia exigidos en el anuncio de licitación o en la invitación a participar en el procedimiento y detallados en los pliegos del contrato. En defecto de estos, la acreditación de la solvencia se efectuará con los requisitos y por los medios que reglamentariamente se establezcan en función de la naturaleza, objeto y valor estimado del contrato, medios y requisitos que tendrán carácter supletorio respecto de los que en su caso figuren en los pliegos.

c) La clasificación no será exigible ni aplicable para los demás tipos de contratos. Para dichos contratos, los requisitos específicos de solvencia exigidos se indicarán en el anuncio de licitación o en la invitación a participar en el procedimiento y se detallarán en los pliegos del contrato. Reglamentariamente se podrán establecer los medios y requisitos que, en defecto de los establecidos en los pliegos, y atendiendo a la naturaleza, objeto y valor estimado del contrato acrediten la solvencia para poder ejecutar estos contratos.»

Cuatro. Se modifican los artículos 75 al 78 del texto refundido de la Ley de Contratos del Sector Público, que quedan redactados de la siguiente manera:

«Artículo 75. *Acreditación de la solvencia económica y financiera.*

1. La solvencia económica y financiera del empresario deberá acreditarse por uno o varios de los medios siguientes, a elección del órgano de contratación:

a) Volumen anual de negocios, o bien volumen anual de negocios en el ámbito al que se refiera el contrato, por importe igual o superior al exigido en el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato o, en su defecto, al establecido reglamentariamente.

b) En los casos en que resulte apropiado, justificante de la existencia de un seguro de indemnización por riesgos profesionales por importe igual o superior al exigido en el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato o, en su defecto, al establecido reglamentariamente.

c) Patrimonio neto, o bien ratio entre activos y pasivos, al cierre del último ejercicio económico para el que esté vencida la obligación de aprobación de cuentas anuales por importe igual o superior al exigido en el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato o, en su defecto, al establecido reglamentariamente.

2. La acreditación documental de la suficiencia de la solvencia económica y financiera del empresario se efectuará mediante la aportación de los certificados y documentos que para cada caso se determinen reglamentariamente. En todo caso, la inscripción en el Registro Oficial de Licitadores y Empresas Clasificadas de las Administraciones Públicas acreditará frente a todos los órganos de contratación del sector público, a tenor de lo en él reflejado y salvo prueba en contrario, las condiciones de solvencia económica y financiera del empresario.

3. En el anuncio de licitación o invitación a participar en el procedimiento y en los pliegos del contrato se especificarán los medios, de entre los recogidos en este artículo, admitidos para la acreditación de la solvencia económica y financiera de los empresarios que opten a la adjudicación del contrato, con indicación expresa del importe mínimo, expresado en euros, de cada uno de ellos. En su defecto, la acreditación de la solvencia económica y financiera se efectuará según lo dispuesto a tales efectos en el apartado 1 del artículo 65 de la Ley.

Artículo 76. *Solvencia técnica en los contratos de obras.*

1. En los contratos de obras, la solvencia técnica del empresario deberá ser acreditada por uno o varios de los medios siguientes, a elección del órgano de contratación:

a) Relación de las obras ejecutadas en el curso de los diez últimos años, avalada por certificados de buena ejecución para las obras más importantes; estos certificados indicarán el importe, las fechas y el lugar de ejecución de las obras y se precisará si se realizaron según las reglas por las que se rige la profesión y se llevaron normalmente a buen término; en su caso, dichos certificados serán comunicados directamente al órgano de contratación por la autoridad competente.

A estos efectos, las obras ejecutadas por una sociedad extranjera filial del contratista de obras tendrán la misma consideración que las directamente ejecutadas por el propio contratista, siempre que este último ostente directa o indirectamente el control de aquélla en los términos establecidos en el artículo 42 del Código de Comercio. Cuando se trate de obras ejecutadas por una sociedad extranjera participada por el contratista sin que se cumpla dicha condición, solo se reconocerá como experiencia atribuible al contratista la obra ejecutada por la sociedad participada en la proporción de la participación de aquél en el capital social de ésta.

b) Declaración indicando los técnicos o las unidades técnicas, estén o no integradas en la empresa, de los que ésta disponga para la ejecución de las obras, especialmente los responsables del control de calidad, acompañada de los documentos acreditativos correspondientes.

c) Títulos académicos y profesionales del empresario y de los directivos de la empresa y, en particular, del responsable o responsables de las obras.

d) En los casos adecuados, indicación de las medidas de gestión medioambiental que el empresario podrá aplicar al ejecutar el contrato.

e) Declaración sobre la plantilla media anual de la empresa y la importancia de su personal directivo durante los tres últimos años, acompañada de la documentación justificativa correspondiente.

f) Declaración indicando la maquinaria, material y equipo técnico del que se dispondrá para la ejecución de las obras, a la que se adjuntará la documentación acreditativa pertinente.

2. En el anuncio de licitación o invitación a participar en el procedimiento y en los pliegos del contrato se especificarán los medios, de entre los recogidos en este artículo, admitidos para la acreditación de la solvencia técnica de los empresarios que opten a la adjudicación del contrato, con indicación expresa, en su caso, de los

valores mínimos exigidos para cada uno de ellos. En su defecto, la acreditación de la solvencia técnica se efectuará según lo dispuesto a tales efectos en el apartado 1 del artículo 65 de la Ley.

Artículo 77. *Solvencia técnica en los contratos de suministro.*

1. En los contratos de suministro la solvencia técnica de los empresarios deberá acreditarse por uno o varios de los siguientes medios, a elección del órgano de contratación:

a) Relación de los principales suministros efectuados durante los cinco últimos años, indicando su importe, fechas y destinatario público o privado de los mismos. Los suministros efectuados se acreditarán mediante certificados expedidos o visados por el órgano competente, cuando el destinatario sea una entidad del sector público o cuando el destinatario sea un comprador privado, mediante un certificado expedido por éste o, a falta de este certificado, mediante una declaración del empresario.

b) Indicación del personal técnico o unidades técnicas, integradas o no en la empresa, de los que se disponga para la ejecución del contrato, especialmente los encargados del control de calidad.

c) Descripción de las instalaciones técnicas, de las medidas empleadas para garantizar la calidad y de los medios de estudio e investigación de la empresa.

d) Control efectuado por la entidad del sector público contratante o, en su nombre, por un organismo oficial competente del Estado en el cual el empresario está establecido, siempre que medie acuerdo de dicho organismo, cuando los productos a suministrar sean complejos o cuando, excepcionalmente, deban responder a un fin particular. Este control versará sobre la capacidad de producción del empresario y, si fuera necesario, sobre los medios de estudio e investigación con que cuenta, así como sobre las medidas empleadas para controlar la calidad.

e) Muestras, descripciones y fotografías de los productos a suministrar, cuya autenticidad pueda certificarse a petición de la entidad del sector público contratante.

f) Certificados expedidos por los institutos o servicios oficiales encargados del control de calidad, de competencia reconocida, que acrediten la conformidad de productos perfectamente detallada mediante referencias a determinadas especificaciones o normas.

2. En los contratos de suministro que requieran obras de colocación o instalación, la prestación de servicios o la ejecución de obras, la capacidad de los operadores económicos para prestar dichos servicios o ejecutar dicha instalación u obras podrá evaluarse teniendo en cuenta especialmente sus conocimientos técnicos, eficacia, experiencia y fiabilidad.

3. En el anuncio de licitación o invitación a participar en el procedimiento y en los pliegos del contrato se especificarán los medios, de entre los recogidos en este artículo, admitidos para la acreditación de la solvencia técnica de los empresarios que opten a la adjudicación del contrato, con indicación expresa, en su caso, de los valores mínimos exigidos para cada uno de ellos y, en su caso, de las normas o especificaciones técnicas respecto de las que se acreditará la conformidad de los productos. En su defecto, la acreditación de la solvencia técnica se efectuará según lo dispuesto a tales efectos en el apartado 1 del artículo 65 de la Ley.

Artículo 78. *Solvencia técnica o profesional en los contratos de servicios.*

1. En los contratos de servicios, la solvencia técnica o profesional de los empresarios deberá apreciarse teniendo en cuenta sus conocimientos técnicos, eficacia, experiencia y fiabilidad, lo que deberá acreditarse, según el objeto del contrato, por uno o varios de los medios siguientes, a elección del órgano de contratación:

a) Una relación de los principales servicios o trabajos realizados en los últimos cinco años que incluya importe, fechas y el destinatario, público o privado, de los mismos. Los servicios o trabajos efectuados se acreditarán mediante certificados

expedidos o visados por el órgano competente, cuando el destinatario sea una entidad del sector público; cuando el destinatario sea un sujeto privado, mediante un certificado expedido por éste o, a falta de este certificado, mediante una declaración del empresario; en su caso, estos certificados serán comunicados directamente al órgano de contratación por la autoridad competente.

b) Indicación del personal técnico o de las unidades técnicas, integradas o no en la empresa, participantes en el contrato, especialmente aquéllos encargados del control de calidad.

c) Descripción de las instalaciones técnicas, de las medidas empleadas por el empresario para garantizar la calidad y de los medios de estudio e investigación de la empresa.

d) Cuando se trate de servicios o trabajos complejos o cuando, excepcionalmente, deban responder a un fin especial, un control efectuado por el órgano de contratación o, en nombre de éste, por un organismo oficial u homologado competente del Estado en que esté establecido el empresario, siempre que medie acuerdo de dicho organismo. El control versará sobre la capacidad técnica del empresario y, si fuese necesario, sobre los medios de estudio y de investigación de que disponga y sobre las medidas de control de la calidad.

e) Las titulaciones académicas y profesionales del empresario y del personal directivo de la empresa y, en particular, del personal responsable de la ejecución del contrato.

f) En los casos adecuados, indicación de las medidas de gestión medioambiental que el empresario podrá aplicar al ejecutar el contrato.

g) Declaración sobre la plantilla media anual de la empresa y la importancia de su personal directivo durante los tres últimos años, acompañada de la documentación justificativa correspondiente.

h) Declaración indicando la maquinaria, material y equipo técnico del que se dispondrá para la ejecución de los trabajos o prestaciones, a la que se adjuntará la documentación acreditativa pertinente.

i) Indicación de la parte del contrato que el empresario tiene eventualmente el propósito de subcontratar.

2. En el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos del contrato se especificarán los medios, de entre los recogidos en este artículo, admitidos para la acreditación de la solvencia técnica de los empresarios que opten a la adjudicación del contrato, con indicación expresa, en su caso, de los valores mínimos exigidos para cada uno de ellos, y en los casos en que resulte de aplicación, con especificación de las titulaciones académicas o profesionales, de los medios de estudio e investigación, de los controles de calidad, de los certificados de capacidad técnica, de la maquinaria, equipos e instalaciones, y de los certificados de gestión medioambiental exigidos. En su defecto, la acreditación de la solvencia técnica o profesional se efectuará según lo dispuesto a tales efectos en el apartado 1 del artículo 65 de la Ley.»

Cinco. Se introduce un nuevo artículo 79 bis en el texto refundido de la Ley de Contratos del Sector Público, con la siguiente redacción:

«Artículo 79 bis. *Concreción de los requisitos y criterios de solvencia.*

La concreción de los requisitos mínimos de solvencia económica y financiera y de solvencia técnica o profesional exigidos para un contrato, así como de los medios admitidos para su acreditación, se determinará por el órgano de contratación y se indicará en el anuncio de licitación o en la invitación a participar en el procedimiento y se detallará en los pliegos, en los que se concretarán las magnitudes, parámetros o ratios y los umbrales o rangos de valores que determinarán la admisión o exclusión de los licitadores o candidatos. En su ausencia serán de aplicación los establecidos reglamentariamente para el tipo de contratos correspondiente, que tendrán igualmente carácter supletorio para los no concretados en los pliegos.

En todo caso, la clasificación del empresario en un determinado grupo o subgrupo se tendrá por prueba bastante de su solvencia para los contratos cuyo objeto esté incluido o se corresponda con el ámbito de actividades o trabajos de dicho grupo o subgrupo, y cuyo importe anual medio sea igual o inferior al correspondiente a su categoría de clasificación en el grupo o subgrupo. A tal efecto, en el anuncio de licitación o en la invitación a participar en el procedimiento y en los pliegos deberá indicarse el código o códigos del Vocabulario «Común de los Contratos Públicos» (CPV) correspondientes al objeto del contrato, los cuales determinarán el grupo o subgrupo de clasificación, si lo hubiera, en que se considera incluido el contrato.

Reglamentariamente podrá eximirse la exigencia de acreditación de la solvencia económica y financiera o de la solvencia técnica o profesional para los contratos cuyo importe no supere un determinado umbral.»

Seis. Se añade una disposición adicional primera bis al texto refundido de la Ley de Contratos del Sector Público con la siguiente redacción:

«Disposición adicional primera bis. *Régimen de contratación de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos.*

Los órganos competentes del Congreso de los Diputados, del Senado, del Consejo General del Poder Judicial, del Tribunal Constitucional, del Tribunal de Cuentas, del Defensor del Pueblo, de las Asambleas Legislativas de las Comunidades Autónomas y de las instituciones autonómicas análogas al Tribunal de Cuentas y al Defensor del Pueblo ajustarán su contratación a las normas establecidas en esta Ley para las Administraciones Públicas.

Asimismo, los órganos competentes de las Cortes Generales establecerán, en su caso, el órgano que deba conocer, en su ámbito de contratación, del recurso especial regulado en el Capítulo VI del Título I del Libro I de esta Ley, respetando las condiciones de cualificación, independencia e inamovilidad previstas en dicho Capítulo.»

Siete. Modificación del apartado f) de la disposición adicional decimosexta del Real Decreto Legislativo 3/2011, por el cual se aprueba el texto refundido de la Ley de Contratos del Sector Público:

«f) Todos los actos y manifestaciones de voluntad de los órganos administrativos o de las empresas licitadoras o contratistas que tengan efectos jurídicos y se emitan a lo largo del procedimiento de contratación deben ser autenticados mediante una firma electrónica avanzada reconocida de acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica. Los medios electrónicos, informáticos o telemáticos empleados deben poder garantizar que la firma se ajusta a las disposiciones de esta norma.

No obstante lo anterior, las facturas electrónicas que se emitan en los procedimientos de contratación se regirán en este punto por lo dispuesto en la Ley 25/2013 de impulso de la factura electrónica y creación del registro contable de facturas en el sector público.»

Ocho. Se modifica la disposición transitoria cuarta del texto refundido de la Ley de Contratos del Sector Público, que queda redactada de la siguiente manera:

«Disposición transitoria cuarta. *Determinación de los casos en que es exigible la clasificación de las empresas y de los requisitos mínimos de solvencia.*

El apartado 1 del artículo 65, en cuanto delimita el ámbito de aplicación y de exigibilidad de la clasificación previa, entrará en vigor conforme a lo que se establezca en las normas reglamentarias de desarrollo de esta Ley por las que se definan los grupos, subgrupos y categorías en que se clasificarán los contratos de obras y los contratos de servicios, continuando vigente, hasta entonces, el párrafo primero del apartado 1 del artículo 25 del Texto Refundido de la Ley de Contratos de las Administraciones Públicas.

La nueva redacción que la Ley de Impulso de la Factura Electrónica y creación del Registro Contable de Facturas en el Sector Público da a los artículos 75, 76, 77 y 78 del texto refundido de la Ley de Contratos del Sector Público y el artículo 79. bis de dicho texto refundido entrarán en vigor conforme a lo que se establezca en las normas reglamentarias de desarrollo de esta Ley por las que se definan los requisitos, criterios y medios de acreditación que con carácter supletorio se establezcan para los distintos tipos de contratos.

No obstante lo anterior, no será exigible la clasificación en los contratos de obras cuyo valor estimado sea inferior a 500.000 euros ni en los contratos de servicios cuyo valor estimado sea inferior a 200.000 euros.»

Disposición final cuarta. *Modificación de la Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización.*

Uno. Se modifica la letra d) de la disposición derogatoria, que queda redactada del siguiente modo:

«d) Las letras a) a e), ambas incluidas, del apartado Uno del artículo 5, las letras a) y b) del apartado Dos y el apartado Tres del Real Decreto-ley 13/2010, de 3 de diciembre, de actuaciones en el ámbito fiscal, laboral y liberalizadoras para fomentar la inversión y la creación de empleo.»

Dos. Se modifica la letra g) de la disposición final decimotercera, que queda redactada del siguiente modo:

«g) Lo previsto en el artículo 35, relativo al importe exigido para la cifra mínima del capital social desembolsado y de recursos propios computables de las sociedades de garantía recíproca, entrará en vigor a los 9 meses de su publicación en el “Boletín Oficial del Estado”.»

Disposición final quinta. *Título competencial.*

La presente Ley tiene carácter básico y se dicta al amparo de los artículos 149.1.6.ª, 149.1.8.ª, 149.1.13.ª, 149.1.14.ª y 149.1.18.ª de la Constitución española.

Disposición final sexta. *Desarrollo reglamentario.*

Reglamentariamente, el Ministro de Hacienda y Administraciones Públicas determinará los requisitos técnicos y funcionales tanto del registro contable de facturas como del punto general de entrada de facturas electrónicas, con el fin de garantizar la integridad, seguridad e interoperabilidad de los distintos sistemas.

Disposición final séptima. *Habilitación normativa.*

Se habilita al Gobierno, al Ministro de Hacienda y Administraciones Públicas y al Ministro de Industria, Energía y Turismo, en el ámbito de sus competencias, a dictar las disposiciones reglamentarias y adoptar medidas necesarias para el desarrollo, la aplicación y ejecución de lo dispuesto en esta Ley.

Disposición final octava. *Entrada en vigor.*

La presente Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado». No obstante:

a) El artículo 4, sobre obligaciones de presentación de factura electrónica, entrará en vigor el 15 de enero de 2015.

b) El artículo 9, sobre anotación en el registro contable de facturas, y la disposición final primera, por la que se modifica el apartado 4 del artículo 34 de la Ley 29/1987, de 18 de diciembre, del Impuesto sobre Sucesiones y Donaciones, entrará en vigor el 1 de enero de 2014.

§ 48

Orden HAP/1074/2014, de 24 de junio, por la que se regulan las condiciones técnicas y funcionales que debe reunir el Punto General de Entrada de Facturas Electrónicas

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 154, de 25 de junio de 2014
Última modificación: 12 de julio de 2016
Referencia: BOE-A-2014-6662

En virtud de la Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, se acomete una de las reformas estructurales que permitirá agilizar los procedimientos de pago al proveedor y dar certeza de las facturas pendientes de pago existentes, con el fin último de reducir la morosidad de las Administraciones Públicas y así contribuir a mejorar la competitividad de las empresas.

Para fortalecer esta necesaria protección del proveedor, se facilita su relación con las Administraciones Públicas favoreciendo el uso de la factura electrónica, su gestión y tramitación telemática, con un mejor control contable de las facturas recibidas por las Administraciones, lo cual permitirá no sólo hacer un mejor seguimiento del cumplimiento de los compromisos de pago de las mismas, sino también, un mejor control del gasto público y del déficit, lo que generará una mayor confianza en las cuentas públicas.

En su artículo 4 la Ley 25/2013, de 27 de diciembre, prevé la creación de un registro contable, que ha sido objeto de desarrollo por la Orden ministerial HAP/492/2014, de 27 de marzo, por la que se regulan los requisitos funcionales y técnicos del registro contable de facturas de las entidades del ámbito de aplicación de la Ley 25/2013, de 27 de marzo.

Para alcanzar estos fines, esta Orden incluye, entre otras medidas dirigidas a mejorar la protección de los proveedores, que cada una de las Administraciones Públicas, estatal, autonómica y local, disponga de puntos generales de entrada de facturas electrónicas para que los proveedores puedan presentarlas y lleguen electrónicamente a la oficina contable competente para que desde la misma se pueda remitir al órgano administrativo al que corresponda su tramitación. De este modo habría un punto general de entrada de facturas electrónicas por cada nivel administrativo, salvo que las Comunidades Autónomas o las Entidades Locales, en aplicación del principio de eficiencia, se adhieran gratuitamente al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado de acuerdo con lo dispuesto en esta Orden. No obstante, aquellas Administraciones Públicas que deseen disponer de su propio Punto General de Entrada, deberán justificar previamente a la realización de cualquier inversión dirigida al establecimiento de su propio punto, su no adhesión al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado.

En uso de la habilitación legal de la disposición final sexta de la Ley 25/2013, de 27 de diciembre, la presente orden ministerial determina los requisitos técnicos y funcionales de los

puntos generales de entrada de facturas electrónicas con carácter básico y, en particular, pone en funcionamiento el servicio FACe, Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado que servirá como punto de intermediación entre quien presenta la factura y la oficina contable competente para su registro, así como las normas de adhesión al mismo por parte de las Comunidades Autónomas y Corporaciones Locales.

La presente Orden se estructura en tres capítulos, dos disposiciones adicionales, dos disposiciones transitorias, tres disposiciones finales y un Anexo. El Capítulo I, establece el objeto y ámbito de aplicación de dicha Orden. El Capítulo II, se refiere a las condiciones técnicas que han de cumplir los puntos generales de entradas de facturas electrónicas y el Capítulo III regula las condiciones funcionales que deben observar tales puntos.

La presente Orden tiene carácter básico, salvo lo dispuesto en la disposición adicional primera que tiene carácter exclusivo y se dicta al amparo del artículo 149.1.13.ª, 14.ª y 18.ª de la Constitución Española, siendo aplicable a todas las Administraciones Públicas y entes, organismos y entidades vinculados o dependientes, que deberán ajustarse a las condiciones y requisitos formales y técnicas establecidos en la misma, así como en desarrollo de la disposición final tercera de la Ley 25/2013, de 27 de diciembre.

En su virtud, de acuerdo con el Consejo de Estado, dispongo:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Orden tiene por objeto determinar los requisitos técnicos y funcionales de los puntos generales de entradas de facturas electrónicas que puedan crear las Comunidades Autónomas y las Entidades Locales, en el caso de no adherirse al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado según el procedimiento del artículo 9 de esta Orden, así como regular tales requisitos respecto del Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado.

Artículo 2. *Ámbito de aplicación.*

Lo previsto en esta Orden será de aplicación a las facturas electrónicas emitidas por los proveedores de bienes y servicios en sus relaciones jurídicas con las Administraciones Públicas en el marco de lo establecido en la Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro Contable de facturas en el Sector Público.

CAPÍTULO II

Requisitos técnicos de los Puntos Generales de Entradas de Facturas Electrónicas

Artículo 3. *Presentación de facturas electrónicas.*

1. Los proveedores de bienes y servicios que deban remitir una factura electrónica a las Administraciones Públicas y a sus entidades, entes y organismos vinculados o dependientes deberán hacerlo a través de los puntos generales de entrada de facturas electrónicas que correspondan.

2. La presentación de facturas por el proveedor a través de este servicio, podrá realizarse mediante un representante del proveedor si así lo permite la normativa específica, o en su defecto, la normativa reguladora de las obligaciones de facturación, y en todo caso, de conformidad con lo previsto en la normativa que resulte aplicable.

3. La presentación de facturas electrónicas a través de los puntos generales de entrada de facturas electrónicas podrá hacerse de dos formas:

a) Individualmente, por medio de un portal web. En este supuesto, la persona que presente la factura habrá de estar en posesión de un certificado electrónico reconocido de persona física, de persona física representante de persona jurídica, o de persona jurídica,

emitido por un prestador de servicios de certificación que figure en la lista de servicios de confianza publicada por el Ministerio de Industria, Energía y Turismo, en cumplimiento de la Decisión de la Comisión 767/2009/CE, de 16 de octubre, por la que se adoptan medidas que facilitan el uso de procedimientos por vía electrónica a través de ventanillas únicas con arreglo a la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior.

b) Electrónicamente, mediante un sistema de comunicación establecido por interfaces de servicios web, que posibilita el envío automático de facturas electrónicas a dicho servicio desde el sistema de gestión de facturas del proveedor. En este supuesto, el sistema de gestión económica del proveedor deberá reunir las condiciones necesarias para su funcionamiento de manera integrada con la interfaz de servicios web de los puntos generales de entrada de facturas electrónicas.

4. Las comunicaciones, a las que se refiere el apartado 3 letra b), entre el sistema del proveedor y el servicio estarán siempre firmadas por un certificado propiedad del proveedor o propiedad de un tercero diferente del proveedor con el que tenga contratado el servicio de facturación electrónica emitido por un prestador de servicios de certificación que figure en la lista de servicios de confianza publicada por el Ministerio de Industria, Energía y Turismo, en cumplimiento de la Decisión 767/2009 de la Comisión Europea.

5. En los supuestos en que la factura electrónica no se ajuste al formato establecido en el artículo 5 de esta Orden o en el caso de que la firma electrónica en dicha factura no cumpla con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, el punto general de entrada de facturas electrónicas la rechazará de forma automática con la correspondiente comunicación al interesado indicando el motivo de dicho rechazo.

Artículo 4. *Procedimiento de remisión de las facturas al correspondiente registro contable de facturas.*

1. Las facturas electrónicas presentadas en los puntos generales de entrada de facturas electrónicas, serán puestas a disposición o remitidas electrónicamente, mediante un servicio proporcionado por dichos puntos a la oficina contable competente para la anotación en el registro contable de la factura. En la factura deberá identificarse los órganos administrativos a los que vaya dirigida de conformidad con la disposición adicional trigésima tercera del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre.

2. La información a poner a disposición o a remitir por cada factura será la propia factura electrónica, el número de asiento registral asignado en el registro asociado al punto general de entrada de facturas electrónicas y la fecha y hora de dicho asiento registral.

3. El registro contable de facturas comunicará al punto general de entrada de facturas electrónicas el código de identificación asignado a la factura en dicho registro.

Artículo 5. *Formato de las facturas.*

1. A efectos de su tratamiento por los puntos generales de entrada de facturas electrónicas, las facturas se ajustarán a lo establecido en el artículo 5 y en la disposición adicional segunda de la Ley 25/2013, de 27 de diciembre.

2. Será obligatorio el uso de una serie de campos dentro de la propia factura para la correcta remisión a los destinatarios así como cumplir con una serie de especificaciones que se detallan en el Anexo que acompaña a esta Orden.

3. El tamaño máximo de una factura electrónica con extensiones e información anexa no deberá ser superior a 8 MB.

Artículo 5 bis. *Extensiones de la factura electrónica.*

1. Las extensiones de la factura electrónica son fragmentos adicionales de información estructurada, añadidos a aquélla, con un esquema propio distinto al de dicha factura.

2. A los efectos de esta Orden se consideran como únicas extensiones válidas en la factura electrónica las sectoriales, que serán aquéllas cuya iniciativa corresponde a un sector de actividad, y cuya aprobación se efectuará en los términos establecidos en el apartado 3 de este artículo.

3. Las extensiones sectoriales se ajustarán a lo establecido en este apartado.

a) La propuesta de extensión sectorial, así como de las modificaciones y bajas de extensiones sectoriales aprobadas, podrá ser formulada, a razón de una única extensión por sector, por la asociación o asociaciones más representativas de cada sector y será dirigida a la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas, utilizando los medios y el procedimiento que al efecto establezca dicha Secretaría de Estado en el portal web del Punto General de Entrada de facturas electrónicas de la Administración General del Estado (FACe).

b) La propuesta de extensión sectorial de "Facturae" deberá incluir una memoria justificativa en la que se proponga y justifique el alcance de la propuesta así como su conveniencia, el XSD de la extensión y un XSLT que permita generar, a partir de la extensión de "Facturae", un documento legible para humanos. Asimismo la memoria incluirá la relación de asociaciones proponentes de la extensión sectorial justificando su representatividad dentro del sector.

Tanto el XSD de una extensión de "Facturae" como el correspondiente XSLT serán de uso libre y gratuito, y de código abierto. El formato del documento legible que se genere con el XSLT deberá ser HTML o PDF.

c) La aprobación o, en su caso, la modificación o baja de la extensión sectorial se realizará por resolución conjunta del Secretario de Estado de Administraciones Públicas y del Secretario de Estado de Presupuestos y Gastos, previo informe preceptivo del Comité Sectorial de la Administración Electrónica, de la Intervención General de la Administración del Estado y de la Dirección General del Patrimonio del Estado.

En la decisión sobre la aprobación o modificación de la extensión sectorial se tendrá en cuenta la representatividad de las asociaciones proponentes, que la información contenida en la extensión sea la requerida por la Administración, y la calidad técnica de la propuesta. En la decisión sobre la baja de la extensión sectorial se tendrá en cuenta la representatividad de las asociaciones proponentes y las razones argumentadas en la memoria.

d) Las extensiones sectoriales aprobadas, como máximo una por sector, y la documentación constitutiva de las mismas se publicarán, con indicación de su fecha de obligatoriedad, que no podrá ser superior a sesenta días desde su fecha de publicación, en el portal web del Punto General de Entrada de facturas electrónicas de la Administración General del Estado (FACe). Los demás puntos generales de entrada de facturas electrónicas deberán contener un enlace a la página web del portal de FACe donde se encuentren las extensiones de "Facturae" aprobadas.

La fecha concreta de obligatoriedad de la extensión aprobada será aquélla a partir de la cual las Administraciones públicas deberán aceptar facturas electrónicas con dicha extensión a través de los puntos generales de entrada de facturas electrónicas, y los emisores de las facturas deberán incluirla.

4. Las facturas electrónicas que contengan extensiones sectoriales no aprobadas en los términos de los apartados anteriores serán rechazadas por el punto general de entrada de facturas electrónicas al que hayan sido enviadas.

5. Únicamente tendrán la consideración de extensiones de "Facturae", a efectos de lo dispuesto en esta Orden, las que se aprueben de conformidad con lo previsto en este artículo.

Artículo 5 ter. *Información anexa.*

Se admitirá información anexa de la factura electrónica como información en la propia factura electrónica o como fichero anexo, en formato no estructurado, PDF o HTML, adicional a la que permite el esquema de datos explícito de la factura electrónica. Se trata de información complementaria a la propia de la factura electrónica que explica, justifica o detalla la información contenida en la misma.

Artículo 6. *Seguimiento y cambio de situación de la factura.*

1. Cuando un proveedor consulte el estado de tramitación de cualquiera de sus facturas, el punto general de entrada de facturas electrónicas correspondiente devolverá el estado que le notifique la oficina contable destinataria directa de la factura electrónica.

2. El proveedor podrá solicitar la retirada de una factura presentada a través del punto general de entrada de facturas electrónicas correspondiente, siempre que se cumplan los requisitos que, en su caso, establezca la normativa reguladora de las obligaciones de facturación.

Artículo 7. *Interoperabilidad del servicio con los sistemas de facturación de los proveedores.*

1. Los puntos generales de entrada de facturas electrónicas proporcionan a los proveedores que deseen automatizar el envío de facturas una interfaz de servicios web, con la cual podrán remitir de forma automática desde sus sistemas de gestión económica las facturas que desean presentar a la Administración a través de aquel servicio.

2. La interfaz permitirá el envío de facturas así como la consulta del estado de las facturas.

CAPÍTULO III

Requisitos funcionales de los Puntos Generales de Entradas de Facturas electrónicas

Artículo 8. *Establecimiento de los Puntos Generales de Entrada de Facturas Electrónicas.*

1. Las Comunidades Autónomas y las Entidades Locales dispondrán de un punto general de entrada de facturas electrónicas a través del cual se recibirán todas las facturas electrónicas que correspondan a entidades, entes y organismos vinculados o dependientes.

2. En cumplimiento de la obligación de establecer un punto general de entrada de facturas electrónicas, las Comunidades Autónomas y Entidades Locales podrán adherirse al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado, de conformidad con lo dispuesto en el siguiente artículo.

3. Aquellas Comunidades Autónomas y Entidades Locales, que creen su propio punto general de entrada de facturas electrónicas, deberán ajustarse a lo dispuesto en esta Orden y justificar ante la Secretaría de Estado de Administraciones Públicas, previamente a la realización de cualquier inversión dirigida al establecimiento de su propio punto de entrada, su no adhesión al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado, en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

En todo caso, se dará publicidad, en sus correspondientes Boletines oficiales de la creación de dichos puntos.

4. Toda factura presentada a través de los puntos generales de entrada de facturas autonómicos o locales producirá una entrada automática en el correspondiente registro electrónico de la Administración Autonómica o de la Entidad local de que se trate, proporcionando un acuse de recibo electrónico con acreditación de la fecha y hora de presentación.

Artículo 8 bis. *Directorio de puntos de entrada de facturas electrónicas de las Administraciones Públicas.*

1. El Directorio de puntos de entrada de facturas electrónicas de las Administraciones Públicas será accesible desde la web face.gob.es y estará, asimismo, enlazado desde la web de "Facturae".

2. Mediante un sistema electrónico articulado a través de los portales de gestión de usuarios de la Secretaría de Estado de las Administraciones Públicas, se llevará a cabo la gestión de usuarios y la actualización de la información del citado directorio por aquellos responsables designados, a tales efectos, por las Administraciones Públicas.

3. La información que con carácter obligatorio deberá constar en dicho directorio para cada una de las Administraciones Públicas será la siguiente:

a) Indicación de su punto general de entrada de facturas electrónicas. En el caso de estar adherida a FACe y además disponer de un punto autonómico o local distinto de FACe, en adelante "punto propio", se consignarán los datos de ambos.

b) Dirección electrónica de su punto propio de entrada de facturas electrónicas. Esta dirección no podrá ser una página genérica sino que enlazará con la dirección en la que el proveedor podrá presentar las facturas a través de una página web.

c) Direcciones de los servicios web de presentación de facturas de forma automática.

d) Dirección de la página informativa o que contenga los manuales de uso del punto general de entrada de facturas electrónicas que corresponda, en su caso.

e) Canales de soporte y atención a proveedores: al menos uno de los siguientes ha de señalarse de forma obligatoria: correo electrónico, formulario web, o teléfono.

f) Indicación de si se aplica la exclusión reglamentaria de la obligación de presentación de factura electrónica prevista en el artículo 4 de la Ley 25/2013, de 27 de diciembre, por importe de facturas, especificando, en caso de aplicación, el límite fijado, y respecto a proveedores a los servicios en el exterior de las Administraciones Públicas.

Artículo 9. *Adhesión de las Comunidades Autónomas y de las Entidades Locales.*

De conformidad con lo establecido en el artículo 6.1 de la Ley 25/2013, de 27 de diciembre, las Comunidades Autónomas y las Entidades Locales podrán adherirse, por medios telemáticos a través del portal electrónico establecido al efecto por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, a la utilización del FACE, Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado que se regula en la disposición adicional primera de la presente Orden. Dicha adhesión, se realizará, en el caso de dicho Punto General de Entrada de Facturas Electrónicas, conforme a las condiciones de uso que se establezcan por resolución del Secretario de Estado de Administraciones Públicas.

Artículo 10. *Asiento Registral en el Registro correspondiente.*

1. Las facturas presentadas a través del punto general de entrada de facturas electrónicas que corresponda serán registradas automáticamente en el registro propio del órgano administrativo competente.

Dicho registro proporcionará un justificante de la presentación de la factura ante el mismo que incluirá el número de registro asignado por el registro electrónico correspondiente.

2. La recepción de facturas en el punto general de entrada de facturas electrónicas correspondiente tendrá únicamente los efectos que, de acuerdo con lo dispuesto en la Ley 25/2013, de 27 de diciembre, se deriven de la presentación de las mismas en un registro administrativo.

Artículo 11. *Uso de la información de los Puntos Generales de Entrada de Facturas Electrónicas.*

La información de los puntos generales de entrada de facturas electrónicas podrá ser utilizada a los efectos de lo dispuesto en el artículo 6.1 de esta Orden. Cuando el punto general de entrada de facturas electrónicas sea utilizado para archivo y custodia de las facturas electrónicas, su información no podrá ser empleada para la explotación o cesión de la información, salvo por el propio órgano administrativo al que corresponda la factura. Ello se entenderá sin perjuicio de las obligaciones que se puedan derivar de la normativa tributaria y de su uso para fines estadísticos.

Disposición adicional primera. *Punto de Entrada de Facturas Electrónicas de la Administración General del Estado.*

1. El Punto de Entrada de Facturas Electrónicas de la Administración General del Estado denominado FACe Punto General de Entrada de Facturas Electrónicas, se ajustará a las condiciones y requisitos funcionales y técnicos establecidos en la presente Orden con las particularidades que se indican a continuación:

a) Recibirá obligatoriamente todas las facturas electrónicas que correspondan a entidades, entes y organismos vinculados o dependientes de la Administración General del

Estado de acuerdo al ámbito de aplicación establecido en la Ley 25/2013, de 27 de diciembre.

b) También recibirá las facturas de entidades, entes y organismos que no perteneciendo al ámbito de la Administración General del Estado, voluntariamente se adhieran al FACe-Punto General de Entrada de Facturas Electrónicas.

c) Toda factura presentada a través del FACe-Punto General de Entrada de Facturas Electrónicas producirá una entrada automática en el registro electrónico común, proporcionando un acuse de recibo electrónico con acreditación de la fecha y hora de presentación.

d) Proporcionará un servicio automatizado de puesta a disposición de las mismas a las oficinas contables competentes para su registro.

e) A través del FACe-Punto General de Entrada de Facturas Electrónicas el proveedor podrá consultar el estado de tramitación de sus facturas electrónicas.

El FACe Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado actualizará de forma permanente el catálogo de unidades administrativas implicadas en la gestión de las facturas electrónicas: oficinas contables, órganos gestores y unidades tramitadoras, y de las asociaciones entre ellas. Esta actualización podrá realizarse directamente en dicho servicio o, preferentemente, mediante sincronización a partir de la información que provean al efecto los registros contables de facturas. Las Comunidades Autónomas y Entidades Locales adheridas al FACE Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado estarán obligadas a mantener permanentemente actualizado el catálogo de unidades administrativas implicadas en la gestión de las facturas electrónicas de sus respectivos ámbitos, incluyendo en el mismo la totalidad de organismos involucrados en este proceso. El servicio FACe no admitirá facturas electrónicas que no correspondan a unidades administrativas que no estén convenientemente reflejadas en los catálogos anteriores.

Si las unidades tramitadoras no dispusieran de medios adecuados para el tratamiento de las facturas electrónicas, se lo comunicarán a la oficina contable correspondiente, a efectos de no dar de alta en el catálogo de unidades administrativas del servicio FACe a aquellas unidades tramitadoras que no dispongan de los medios o del sistema de gestión económica que permita la gestión y almacenamiento de las facturas electrónicas.

2. El órgano competente para la gestión, administración y mantenimiento del FACe-Punto General de Entrada de Facturas Electrónicas es la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas.

Corresponde a este centro directivo determinar las condiciones técnicas de uso de dicho Punto General, oído el Consejo Superior de Administración Electrónica, que estarán publicadas en su propio portal electrónico.

No obstante lo anterior, la determinación, en su caso, de las condiciones técnicas normalizadas de las interfaces del Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado con otros puntos de entradas de facturas electrónicas, sistemas y plataformas emisores o receptores de las facturas electrónicas, corresponderá conjuntamente a las Secretarías de Estado de Administraciones Públicas y de Presupuestos y Gastos, oído el Consejo Superior de Administración Electrónica.

3. La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica publicará la última versión de dicha interfaz en el Centro de Transferencia de Tecnología en la siguiente dirección web: http://administracionelectronica.gob.es/es/ctt/face. Además proporcionará un entorno de pruebas a los proveedores para que realicen las pruebas que sean necesarias en aras de la integración completa de sus sistemas con este servicio.

4. Se excluye de la presentación obligatoria en FACe-Punto General de Entrada de Facturas Electrónica a las facturas electrónicas por importe de hasta 5.000 euros y a las facturas electrónicas emitidas por proveedores a los servicios en el exterior hasta que se haya consolidado el uso de la factura electrónica y los servicios en el exterior dispongan de los medios y sistemas apropiados para su recepción en dichos servicios.

5. Las facturas presentadas a través del FACe-Punto General de Entrada de Facturas Electrónicas serán registradas automáticamente en el registro electrónico común, de acuerdo con lo señalado en la Orden HAP/566/2013, de 8 de abril, por la que se regula el Registro Electrónico Común o en el registro electrónico correspondiente a la Administración Pública de que se trate. Dicho servicio proporcionará un justificante de la presentación de la factura ante el mismo que incluirá el número de registro asignado por dicho registro.

Disposición adicional segunda. *No incremento de gasto público.*

Las medidas contenidas en esta Orden se atenderán con los medios personales y materiales existentes en el Ministerio de Hacienda y Administraciones Públicas, y en ningún caso podrá generar incremento de gasto público.

Disposición transitoria única. *Formato transitorio de las facturas.*

En tanto no se apruebe la Orden ministerial a la que se refiere el artículo 5 de esta Orden, las facturas deberán haber sido expedidas en el formato que la Ley 25/2013, de 27 de diciembre, establece en su disposición adicional segunda y estar firmadas con firma electrónica avanzada basada en un certificado reconocido, de acuerdo con lo dispuesto en el artículo 10.1 a) del Reglamento por el que se regulan las obligaciones de facturación, aprobado mediante Real Decreto 1619/2012, de 30 de noviembre, o mediante sello electrónico avanzado basado en un certificado reconocido de los admitidos por la plataforma de verificación del estado de revocación de los certificados admitidos, prevista en el artículo 25.1 del Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

El certificado en el que se base la firma o el sello electrónico avanzado deberá ser alguno de los incluidos en el servicio de publicación del Ministerio de Industria, Energía y Turismo, previsto en el artículo 30.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, y a partir de la fecha de aplicación del Reglamento (UE) 910/2014, de identificación electrónica y servicios de confianza para las transacciones en el mercado interior, en la "Lista de confianza de prestadores de servicios de certificación" (TSL), publicada en la sede electrónica del Ministerio de Industria, Energía y Turismo.

Disposición final primera. *Aplicación y ejecución de la Orden.*

Se habilita al titular de la Secretaría de Estado de Administraciones Públicas, en el ámbito de su competencia, a adoptar las resoluciones y medidas necesarias para la aplicación y ejecución de lo dispuesto en esta Orden, especialmente en relación con las condiciones de uso de FACe Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado.

Disposición final segunda. *Título competencial.*

La presente Orden tiene carácter básico salvo lo dispuesto en la disposición adicional primera y se dicta al amparo del artículo 149.1.13.ª, 14.ª y 18.ª de la Constitución Española.

Disposición final tercera. *Entrada en vigor.*

La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO I

Campos factura

1. De conformidad con lo señalado en el artículo 5 de esta Orden, se deberá incluir una serie de campos dentro de la propia factura para la correcta remisión a los destinatarios. Algunos de estos campos serán cumplimentados con carácter obligatorio en todas las

facturas, y en otros campos, su cumplimentación es opcional, pero en el caso de que se desee informar de los mismos debe utilizarse el campo que se indica.

2. Dentro del documento de factura electrónica será obligatorio, para la correcta remisión de la factura al órgano destinatario final, informar del órgano gestor, la unidad tramitadora y la oficina contable destinatarios. Y opcionalmente, del órgano proponente.

Las unidades deberán ir codificadas bajo la etiqueta de centros administrativos del «» de la factura

ROL	RoleTypeCode	CentreCode	Descripción	Tipo
Fiscal	01	Código de la unidad en DIRECTORIO	Oficina Contable	Obligatorio
Receptor	02	Código de la unidad en DIRECTORIO	Órgano Gestor	Obligatorio
Pagador	03	Código de la unidad en DIRECTORIO	Unidad Tramitadora	Obligatorio
Comprador	04	Código de la unidad en DIRECTORIO	Órgano proponente	Opcional

El código del centro será el código de dicha unidad en el sistema «Directorio Común de Unidades Orgánicas y Oficinas DIR3» recogido en el artículo 9 del Esquema Nacional de Interoperabilidad (Real Decreto 4/2010).

Ejemplo de XML todos los roles de centros administrativos rellenos:

```
- <AdministrativeCentres>
  - <AdministrativeCentre>
      <CentreCode>E00000012</CentreCode>
      <RoleTypeCode>01</RoleTypeCode>
    - <AddressInSpain>
        <Address>Paseo de la Castellana</Address>
        <PostCode>20871</PostCode>
        <Town>Madrid</Town>
        <Province>Madrid</Province>
        <CountryCode>ESP</CountryCode>
      </AddressInSpain>
      <CentreDescription>Oficina Contable</CentreDescription>
    </AdministrativeCentre>
  - <AdministrativeCentre>
      <CentreCode>E00000034</CentreCode>
      <RoleTypeCode>02</RoleTypeCode>
    - <AddressInSpain>
        <Address>Paseo de la Castellana</Address>
        <PostCode>28071</PostCode>
        <Town>Madrid</Town>
        <Province>Madrid</Province>
        <CountryCode>ESP</CountryCode>
      </AddressInSpain>
      <CentreDescription>Órgano Gestor</CentreDescription>
    </AdministrativeCentre>
  - <AdministrativeCentre>
      <CentreCode>E000000033</CentreCode>
      <RoleTypeCode>03</RoleTypeCode>
    - <AddressInSpain>
        <Address>Paseo de la Castellana</Address>
        <PostCode>20871</PostCode>
        <Town>Madrid</Town>
        <Province>Madrid</Province>
        <CountryCode>ESP</CountryCode>
      </AddressInSpain>
      <CentreDescription>Unidad Tramitadora</CentreDescription>
    </AdministrativeCentre>
  - <AdministrativeCentre>
      <CentreCode>E00000023</CentreCode>
      <RoleTypeCode>04</RoleTypeCode>
    - <AddressInSpain>
        <Address>Paseo de la Castellana</Address>
        <PostCode>20871</PostCode>
        <Town>Madrid</Town>
        <Province>Madrid</Province>
        <CountryCode>ESP</CountryCode>
      </AddressInSpain>
      <CentreDescription>Subdirección de compras</CentreDescription>
    </AdministrativeCentre>
  </AdministrativeCentres>
```

ANEXO II

Fichero de datos de carácter personal

Nombre del fichero: «Punto General de Entrada de facturas electrónicas de la AGE»

Finalidad del fichero y usos previstos: Anotación de información necesaria para el control de acceso al estado y gestión de las facturas recibidas en el servicio FACe-Punto General de Entrada de facturas electrónicas de la Administración General del Estado.

Personas o colectivos sobre los que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos: Terceros de las facturas que sean remitidas a los registros contables de facturas de la Administración General del Estado.

Procedimiento de recogida de datos de carácter personal: De los datos del tercero en la propia factura recibida en la Administración General del Estado y de los datos del tercero que presenta la factura.

Estructura básica del fichero y descripción de los tipos de datos de carácter personal, incluidos en el mismo: Se recogerán los siguientes datos personales:

Datos del emisor/proveedor:

Código de identificación fiscal.
Nombre y apellidos.

Datos del firmante de la factura:

Código de identificación fiscal.
Nombre y apellidos.

Datos del presentador de la factura:

Código de identificación fiscal.
Nombre y apellidos.
Correo electrónico.

Datos del cesionario (si lo hubiera):

Código de identificación fiscal.
Nombre y apellidos.

Datos del emisor/tercera persona (si lo hubiera):

Código de identificación fiscal.
Nombre y apellidos.

Sistema de tratamiento: Fichero automatizado.

Comunicaciones previstas de los datos, indicando, en su caso, los destinatarios o categorías de destinatarios: Comunicación de datos a los registros contables de facturas de las Administraciones Públicas destinatarias de las facturas.

Transferencias internacionales previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No previstas.

Órganos responsables del fichero: Subdirección General de Impulso de la Administración Digital y Servicio al Ciudadano de la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas.

Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Impulso de la Administración Digital y Servicio al Ciudadano de la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Hacienda y Administraciones Públicas, calle María de Molina, número 50, 28071, Madrid.

Nivel básico, medio o alto de seguridad: Nivel básico.

ANEXO III

Definiciones

A efectos de esta Orden ministerial, se entenderá por:

1. <<información estructurada>>: Información en formato electrónico compuesta por datos que pueden ser generados y procesados automáticamente por sistemas informáticos.

2. <<información no estructurada>>: Información en formato electrónico cuyo procesamiento para extraer de ella datos que puedan ser procesados automáticamente por los sistemas informáticos del receptor requiere la intervención humana o un proceso costoso que no suele estar completamente automatizado, como el reconocimiento óptico de caracteres (OCR).

3. <<esquema de datos explícito>>: El conjunto de datos que el formato de la factura electrónica define explícitamente. Excluye, por tanto, lo que pueda contener cualquier extensión o anexo de la factura electrónica, sea estructurado o no.

4. <<XSD>>: XML Schema Definition. Documento que describe una estructura específica, a la que se denomina formato, de documento electrónico escrito en un lenguaje informático que se denomina XML. El XSD permite interpretar el documento electrónico. El XSD define también el modelo de datos explícito que corresponde a ese formato. El XSD es, a su vez, un documento electrónico procesable automáticamente por un sistema informático. Un ejemplo de XSD es el XSD "Facturae", que describe como crear facturas escritas en XML conforme al formato "Facturae".

5. << Facturae>>: XSD del formato de factura electrónica "Facturae" que se determina en la disposición adicional segunda de la Ley 25/2013, de 27 de diciembre.

6. <<XSLT>>: Documento electrónico que determina cómo transformar un documento electrónico escrito en XML en otro documento en otro formato legible para humanos.

7. <<Sello electrónico avanzado basado en un certificado reconocido>>: Instrumento para garantizar integridad y autenticidad de un documento electrónico definido en el artículo 5.2 de la Ley 25/2013, de 27 de diciembre, y en el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

8. <<Punto general de entrada>>: Aquel que cumpla con las especificaciones establecidas al respecto en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público, y su normativa de desarrollo.

§ 49

Resolución de 25 de junio de 2014, de la Secretaría de Estado de Administraciones Públicas, por la que se establecen las condiciones de uso de la plataforma FACe-Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 157, de 28 de junio de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-6787

La Comisión para la Reforma de las Administraciones Públicas (CORA) contempla diversas reformas estructurales para mejorar la eficiencia así como erradicar la morosidad de las Administraciones Públicas. Fruto de esas reformas estructurales es la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

En el Preámbulo de la citada Ley, se recoge que uno de los elementos clave para mejorar la competitividad de las empresas consiste en reducir la morosidad de las Administraciones Públicas, ya que esto permitirá, a su vez, reducir sus necesidades de financiación y evitar los efectos negativos que dicha morosidad genera sobre su empleo y su propia supervivencia.

En el artículo 9 de la Orden HAP/1074/2014, de 24 de junio, por la que se regulan las condiciones técnicas y funcionales que debe reunir el punto general de entrada de facturas electrónicas, se señala que la Secretaría de Estado de Administraciones Públicas establecerá los términos en los que se realizará la adhesión de las Comunidades Autónomas y de las Entidades Locales a la utilización del Punto General de Entrada de Facturas Electrónicas que proporcione la Administración General del Estado.

Por todo ello, la Secretaría de Estado de Administraciones Públicas, en el ejercicio de las competencias previstas en el artículo 12 del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, ha resuelto:

1. Ordenar la publicación en el «Boletín Oficial del Estado» de esta Resolución, en cuyo anexo figuran las condiciones de uso del Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado, previsto en la Ley 25/ 2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas electrónicas y en la Orden HAP/1074/2014, de 24 de junio, por la que se regulan las condiciones técnicas y funcionales que debe reunir el punto general de entrada de facturas electrónicas, que se adjuntan como anexo.

2. Las citadas condiciones de uso serán, así mismo, publicadas en la plataforma electrónica FACe http://www.face.gob.es y en el Centro de Transferencia de Tecnología –CTT– de la Administración General del Estado, http://administracionelectronica.gob.es/es/ctt/face.

3. Esta Resolución surtirá efecto a partir del día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Condiciones de uso de la plataforma FACe-Punto general de entrada de facturas electrónicas

I. Las Administraciones Públicas a las que se refiere el artículo 2.2 de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, con la excepción de la Administración General del Estado, y sus organismos y entes dependientes y vinculados, y las entidades gestoras y los servicios comunes de la Seguridad Social, cuando se adhieran a la utilización de la plataforma FACe-Punto General de Entrada de Facturas Electrónicas, en adelante plataforma FACe, se comprometen a aceptar las siguientes condiciones de uso:

a) Según lo dispuesto en la disposición adicional quinta de la Ley 25/2013, de 27 de diciembre, relativa a la adhesión al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado, las Administraciones autonómicas y locales que quieran adherirse a la utilización de la plataforma FACe deberán aceptar y firmar, mediante una firma electrónica avanzada de acuerdo con la Ley 59/2003, de 19 de diciembre, de firma electrónica, el documento de adhesión al Punto General de Entrada de Facturas Electrónicas de la Administración General del Estado a través del portal electrónico establecido al efecto en el citado punto por la Secretaría de Estado de Administraciones Públicas del Ministerio de Hacienda y Administraciones Públicas. No obstante, podrá accederse también a dicho documento de adhesión a través de los portales de Entidades Locales, Comunidades Autónomas y de Gestión Administrativa de la Secretaría de Estado de Administraciones Públicas así como en aquellos portales que la Secretaría de Estado de Administraciones Públicas decida en el futuro.

b) Mantener actualizada la información de sus unidades organizativas implicadas en la gestión de las facturas electrónicas en la plataforma FACe y a responsabilizarse de la gestión de las mismas, de conformidad con la disposición adicional trigésima tercera del texto refundido de la Ley de Contratos del Sector Público, aprobado por el Real Decreto Legislativo 3/2011, de 14 de noviembre.

c) Hacer un uso responsable de la plataforma FACe adecuándose estrictamente a las finalidades recogidas en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público, y en la normativa que de esta se derive, y responsabilizarse del buen uso y gestión de la plataforma así como de cualquier daño y perjuicio directo o indirecto que provenga del mal empleo de la citada plataforma.

d) Acceder a la plataforma bajo los canales que la Secretaría de Estado de Administraciones Públicas establezca. Las comunicaciones de las distintas Administraciones Públicas con el punto se adecuarán a las condiciones técnicas normalizadas que la Secretaría de Estado de Administraciones Públicas y la Secretaría de Estado de Presupuestos y Gastos determinen.

e) Cumplir con las instrucciones técnicas de los manuales de uso de la plataforma FACe, que serán publicadas en el Centro de Transferencia de Tecnología –CTT– de la Administración General del Estado en la siguiente url de la iniciativa FACe del CTT: http://administracionelectronica.gob.es/es/ctt/face.

II. Los proveedores de bienes y servicios que, de acuerdo con lo dispuesto en los artículos 3 y 4 de la Ley 25/2013, de 27 de diciembre, presenten facturas electrónicas a través de la plataforma FACe deberán:

a) Realizar un uso adecuado y responsable de la plataforma FACe.

b) Aceptar la declaración de conformidad, publicada en el portal face.gob.es, e informar a través de la plataforma, de aquellos datos de identificación necesarios para la correcta comunicación entre proveedor y plataforma, tanto de los suyos propios como de las personas que los representen en esta relación.

c) Acceder a la plataforma bajo los canales que la Secretaría de Estado de Administraciones Públicas establezca. Las comunicaciones para la presentación de las facturas electrónicas en el punto se adecuarán a las condiciones técnicas normalizadas que la Secretaría de Estado de Administraciones Públicas y la Secretaría de Estado de Presupuestos y Gastos determinen.

d) Cumplir con las instrucciones técnicas de los manuales de uso de la plataforma FACe, que serán publicadas en el Centro de Transferencia de Tecnología –CTT– de la Administración General del Estado en la siguiente url de la iniciativa FACe del CTT: http://administracionelectronica.gob.es/es/ctt/face.

§ 50

Resolución de 10 de octubre de 2014, de la Secretaría de Estado de Administraciones Públicas y de la Secretaría de Estado de Presupuestos y Gastos, por la que se establecen las condiciones técnicas normalizadas del punto general de entrada de facturas electrónicas

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 255, de 21 de octubre de 2014
Última modificación: sin modificaciones
Referencia: BOE-A-2014-10660

La Comisión para la Reforma de las Administraciones Públicas (CORA) contempla diversas reformas estructurales para mejorar la eficiencia así como erradicar la morosidad de las Administraciones Públicas. Fruto de esas reformas estructurales es la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

En el Preámbulo de la Ley 25/2013, de 27 de diciembre, se recoge que uno de los elementos clave para mejorar la competitividad de las empresas consiste en reducir la morosidad de las Administraciones públicas, ya que esto permitirá, a su vez, reducir sus necesidades de financiación y evitar los efectos negativos que dicha morosidad genera sobre su empleo y su propia supervivencia.

En el artículo 6.6 de la citada Ley, se establece que la Secretaría de Estado de Administraciones Públicas y la Secretaría de Estado de Presupuestos y Gastos determinarán conjuntamente las condiciones técnicas normalizadas del punto general de entrada de facturas electrónicas.

Por todo ello, la Secretaría de Estado de Administraciones Públicas y la Secretaría de Estado de Presupuestos y Gastos, en el ejercicio de las competencias previstas en los artículos 12 y 7, respectivamente, del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, han resuelto:

1. Ordenar la publicación en el Boletín Oficial del Estado de esta Resolución, en cuyo anexo figuran las condiciones técnicas normalizadas del punto general de entrada de facturas electrónicas de la Administración General del Estado, previsto en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas electrónicas en el sector público.

2. Las citadas condiciones técnicas normalizadas así como el desarrollo detallado de cada una de ellas serán publicadas en el portal de administración electrónica de la Administración General del Estado http://administracionelectronica.gob.es.

3. Esta Resolución surtirá efecto a partir del día siguiente al de su publicación en el Boletín Oficial del Estado.

ANEXO

Condiciones técnicas del punto general de entrada de facturas electrónicas

I. Los puntos generales de entrada de facturas electrónicas de las Administraciones Públicas a las que se refiere el artículo 2.2 de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público deberán cumplir las siguientes condiciones técnicas normalizadas en materia de flujos de estados de las facturas electrónicas:

a) Estados de tramitación de las facturas electrónicas del punto general de entrada de facturas electrónicas.

El punto general de entrada de facturas electrónicas recogerá al menos los siguientes estados públicos de tramitación y su codificación:

Nombre público de estado	Código público de estado
Registrada	1200
Registrada en RCF	1300
Contabilizada la obligación reconocida	2400
Pagada	2500
Rechazada	2600
Anulada	3100

Definición de estados:

Registrada: La factura electrónica ha sido recibida en el punto general de entrada de facturas y ha sido registrada administrativamente, proporcionando un número de asiento registral al proveedor.

Registrada en RCF: La factura electrónica ha sido recibida y registrada en el registro contable de facturas de la oficina contable destinataria.

Contabilizada la obligación reconocida: La obligación de pago derivada de la factura ha sido reconocida.

Pagada: La obligación de pago derivada de la factura ha sido pagada.

Rechazada: La oficina contable o la unidad tramitadora han rechazado la factura, se debe indicar al proveedor el motivo del rechazo.

Anulada: La oficina contable o la unidad tramitadora aceptan la solicitud de anulación de la factura electrónica, presentada por el proveedor.

b) Listado de estados de tramitación de la solicitud de anulación de las facturas electrónicas del punto general de entrada de facturas electrónicas.

La solicitud de anulación por parte del proveedor de la factura no paraliza el proceso de tramitación interno de la factura. El punto general de entrada de facturas electrónicas recogerá al menos los siguientes estados de tramitación de la solicitud de anulación y su codificación:

Nombre estado	Código de estado
No solicitada anulación	4100
Solicitada anulación	4200
Aceptada anulación	4300
Rechazada anulación	4400

Definición de estados:

No solicitada anulación: El proveedor no ha solicitado anulación sobre la factura electrónica.

Solicitada anulación: El proveedor solicita anulación de la factura electrónica informando también del motivo.

Aceptada anulación: La unidad tramitadora acepta la solicitud de anulación de la factura electrónica. Cambia automáticamente el estado de tramitación de una factura a Anulada-3100 en el flujo de tramitación.

Rechazada anulación: La unidad tramitadora rechaza la solicitud de anulación de la factura electrónica.

II. Los puntos generales de entrada de facturas electrónicas de las Administraciones Públicas a las que se refiere el artículo 2.2 de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público deberán cumplir las siguientes condiciones técnicas normalizadas en materia de interfaz de servicios web:

a) En su relación con los proveedores de las Administraciones Públicas, la interfaz de servicios web recogida en el artículo 3.3.b de la Orden Ministerial HAP/1074/2014 por la que se regulan las condiciones técnicas y funcionales que debe reunir el Punto General de Entrada de Facturas Electrónicas, deberá cumplir las siguientes especificaciones normalizadas:

Implementar al menos los siguientes métodos:

1. enviarFactura: Método que permitirá al proveedor presentar una factura electrónica en el punto general de entrada de facturas electrónicas. El proveedor puede remitir la factura electrónica y los anexos asociados si los hubiera.
2. consultarEstadoFactura: Partiendo del número de asiento registral dado al proveedor al presentar la factura a través del método EnviarFactura, a través de este método el proveedor que remitió la factura podrá consultar el estado actual de tramitación de su factura.
3. consultarListadoFacturas: Similar al método consultarEstadoFactura pero, en este caso, permitirá consultar el estado de varias facturas de un proveedor a la vez.
4. anularFactura: Método que permitirá al proveedor, indicando el número de asiento registral de la factura asociada y el motivo de anulación, solicitar la anulación de la factura.
5. consultarEstados: Método que devolverá al proveedor el listado de todos los estados públicos de tramitación de la factura electrónica y de la solicitud de anulación de facturas.
6. consultarUnidades: Método que devolverá un listado de todas las unidades que pueden recibir facturas electrónicas dadas de alta en el punto general de entrada de facturas. Se devolverán en el formato de relación oficina contable, órgano gestor y unidad tramitadora.
7. consultarAdministraciones: Método que devolverá el listado de todas las administraciones públicas dadas de alta en el punto general de entrada de facturas electrónicas.
8. consultarUnidadesPorAdministracion: Método que devolverá un listado de todas las unidades de una determinada Administración Pública que pueden recibir facturas electrónicas en el punto general de entrada de facturas. Se devuelven en el formato de relación oficina contable, órgano gestor y unidad tramitadora.

Solo el proveedor que ha presentado una factura electrónica podrá consultar su estado de tramitación y solicitar la anulación de la misma. Para ello será necesario autenticar y autorizar con anterioridad a dicho proveedor.

b) En su relación con los sistemas informáticos de los registros contables de facturas, la interfaz de servicios web recogida en el artículo 3.3.b de la Orden Ministerial HAP/1074/2014 por la que se regulan las condiciones técnicas y funcionales que debe reunir el Punto General de Entrada de Facturas Electrónicas, deberá cumplir las siguientes condiciones técnicas normalizadas en materia de interfaz de servicios web:

Implementar al menos los siguientes métodos, relativos al alta de unidades en el punto general de entrada de facturas electrónicas:

1. solicitudAdhesion: Método que permitirá realizar la gestión de alta, baja, actualización de oficinas contables, órganos gestores y unidades tramitadoras en el punto general de entrada de facturas electrónicas desde los sistemas informáticos de los registros contables de facturas.
2. consultaSolicitudAdhesion: Método que devolverá el estado de la solicitud o solicitudes de alta, baja, actualización de las unidades de una Administración Pública realizadas desde el sistema informático del registro contable de facturas.

3. consultaProcesadoSolicitudAdhesion: Para una solicitud de gestión de unidades dada devolverá el detalle del procesado de dicha solicitud, informando de los errores encontrados.

Implementar al menos los siguientes métodos, relativos a la tramitación de facturas electrónicas:

1. solicitarNuevasFacturas: Método que permitirá consultar al punto general de entrada el listado de las nuevas facturas recibidas en el punto dirigidas a las oficinas contables del registro contable de facturas que realiza la consulta.

2. solicitarNuevasAnulaciones: Método que permitirá consultar al punto general de entrada el listado de solicitudes de anulación de las facturas electrónicas dirigidas a las oficinas contables del registro contable de facturas.

3. descargarFactura: Método que permitirá la descarga, por parte del sistema informático del registro contable de facturas, de una factura electrónica dirigida a una de sus oficinas contables. Este método permitirá la descarga del fichero de la factura electrónica y los ficheros anexos que el proveedor haya incluido en la presentación de la factura en el punto general de entrada.

4. confirmarDescargaFactura: Método que permitirá al sistema informático del registro contable de facturas destinatario de la factura informar al punto general de entrada de facturas que ha recibido correctamente la factura.

5. cambiarEstadoFactura: Método que permitirá al sistema informático del registro contable de facturas destinatario de la factura informar al punto general de entrada del cambio de estado público de la factura.

6. consultarEstados: Método que permitirá al sistema informático del registro contable de facturas conocer el listado de todos los estados de la factura aceptados por el punto general de entrada y el código de cada uno de ellos.

7. consultarUnidades: Método que permitirá al sistema informático del registro contable de facturas conocer qué unidades están asociadas a su sistema informático en el punto general y por tanto de las que podrá solicitar descarga de las facturas recibidas.

8. gestionarSolicitudAnulacionFactura: Método que permitirá al sistema informático del registro contable de facturas informar sobre la aceptación o rechazo de una solicitud de anulación de factura por parte del proveedor.

Desde la parte del receptor de la factura, solo el sistema informático del registro contable de facturas asociado a la oficina contable destinataria de la factura electrónica podrá acceder a dicha factura electrónica y realizar todas las acciones habilitadas sobre dicha factura. Para ello será necesario autenticar y autorizar con anterioridad a dicho sistema informático.

c) Todas las comunicaciones de las interfaces de servicios web implementadas por el punto general de entrada de facturas electrónicas estarán firmadas con un formato válido de WS-Security 1.0 X.509 Token Profile. Este sistema permitirá identificar al proveedor y a la Administración destinataria en sus relaciones, a través de las interfaces de servicios web, con el punto general de entrada de facturas electrónicas.

Ejemplo de petición firmada:

```
<soapenv:Envelope xmlns:soapenv="http://
schemas.xmlsoap.org/soap/envelope/" xmlns:xsd= "http://
www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
<soapenv:Header>
  <wsse:Security soapenv:mustUnderstand="1"
xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/
oasis-200401-wss-wssecurity-secext-1.0.xsd">
    <wsse:BinarySecurityToken EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-
security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3" wsu:Id="CertId-
DD1EB7392FADB1EE3713600719200334" xmlns:wsu="http://
docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">MIIEpDC...</wsse:BinarySecurityToken>
```

```
    <ds:Signature Id="Signature-3" xmlns:ds="http://
www.w3.org/2000/09/xmldsig#">
      <ds:SignedInfo>
        <ds:CanonicalizationMethod Algorithm="http://
www.w3.org/2001/10/xml-exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://
www.w3.org/2000/09/xmldsig#rsa-sha1" />
        <ds:Reference URI="#id-4">
          <ds:Transforms>
            <ds:Transform Algorithm="http://
www.w3.org/2001/10/xml-exc-c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://
www.w3.org/2000/09/xmldsig#sha1" />
          <ds:DigestValue>wttpKeqdo7ltsD2MDitjZ7RWWaM=</
ds:DigestValue>
        </ds:Reference>
      </ds:SignedInfo>
      <ds:SignatureValue>n34z9gC...</ds:SignatureValue>
      <ds:KeyInfo Id="KeyId-DD1EB7392FADB1EE3713600719200345">
        <wsse:SecurityTokenReference wsu:Id="STRId-
DD1EB7392FADB1EE3713600719200346" xmlns:wsu="http://
docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">
          <wsse:Reference URI="#CertId-
DD1EB7392FADB1EE3713600719200334" ValueType="http://
docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-
profile-1.0#X509v3" />
        </wsse:SecurityTokenReference>
      </ds:KeyInfo>
    </ds:Signature>
  </wsse:Security>
</soapenv:Header>
<soapenv:Body wsu:Id="id-4" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">
  <cambiarEstadoFactura xmlns="http://
ssweb.preapp.seap.minhap.es/facturae/web_services.php/ssgg">
    <organoGestor xsi:type="xsd:string" xmlns="">E00127403</
organoGestor>
    <unidadTramitadora xsi:type="xsd:string"
xmlns="">E03062503</unidadTramitadora>
    <numeroRegistro xsi:type="xsd:string"
xmlns="">O00001301_13_00000142</numeroRegistro>
    <codigoEstado xsi:type="xsd:string" xmlns="">1200</
codigoEstado>
    <comentarios xsi:nil="true" xsi:type="xsd:string"
xmlns="" />
  </cambiarEstadoFactura>
</soapenv:Body>
```

§ 51

Orden HAP/492/2014, de 27 de marzo, por la que se regulan los requisitos funcionales y técnicos del registro contable de facturas de las entidades del ámbito de aplicación de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 77, de 29 de marzo de 2014
Última modificación: 6 de agosto de 2015
Referencia: BOE-A-2014-3373

El registro contable de facturas previsto en la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público, pretende ser un instrumento clave para la mejora en los procedimientos contables, a través del control contable riguroso de las facturas recibidas por las Administraciones, a efectos de lograr una mayor confianza en las cuentas públicas y de mejorar el control de la morosidad en las Administraciones públicas. Su puesta en funcionamiento no solamente contribuirá a proporcionar un mejor control del gasto público, sino también a facilitar el seguimiento del cumplimiento de los compromisos de pago de las Administraciones Públicas.

La creación del registro contable de facturas constituye una obligación de cada una de las entidades incluidas en el ámbito de aplicación de la ley 25/2013, de 27 de diciembre, a partir de 1 de enero de 2014. A partir de dicha fecha todas las facturas que se expidan por los servicios prestados o bienes entregados a las citadas entidades, cualquiera que sea su soporte, electrónico o papel, deberán ser objeto de anotación en el correspondiente registro contable de facturas, que estará integrado o interrelacionado con el respectivo sistema de información contable de la entidad u organismo público, y gestionado por el órgano o unidad administrativa que tenga atribuida la función de contabilidad.

Para ello, las facturas recibidas en el registro administrativo deben ser anotadas por el órgano competente en el registro contable de facturas en los términos establecidos por la Ley 25/2013, de 27 de diciembre. Cuando se trate de facturas electrónicas, éstas se recibirán por cada entidad a través del correspondiente Punto general de entrada de facturas electrónicas, con anotación en el respectivo registro electrónico administrativo, para inmediatamente, y de forma automática, ser remitidas al registro contable de facturas que corresponda al centro gestor, entidad u organismo destinatario de la factura.

Las facturas anotadas en el registro contable de facturas serán distribuidas o puestas a disposición de los correspondientes órganos competentes para su tramitación, de acuerdo con la identificación de esos órganos o unidades que figure en la propia factura, a efectos de realizar, si procede, el procedimiento de conformidad con la entrega del bien o la prestación del servicio realizada. El trámite preliminar de aceptación o rechazo de cada factura se

anotará en el registro contable de facturas, dejando constancia de la fecha en que se haya producido, así como, en caso de aprobación de la conformidad y reconocimiento de la obligación, de la fecha de contabilización de la obligación reconocida correspondiente.

Es precisamente esta anotación continua en el registro contable de facturas de los distintos estados por los que vaya pasando la factura, desde su recepción y registro, pasando por la aceptación o rechazo y devolución de la misma por el órgano gestor, su anulación, en su caso, a instancia del presentador de la factura, y, en el caso de aprobación de la conformidad y reconocimiento de la obligación, la contabilización de la obligación reconocida y de su pago, lo que permitirá que el registro contable de facturas se convierta en un instrumento clave para el seguimiento del cumplimiento de los compromisos de pago de las entidades y organismos públicos, a la vez que sea un medio para informar a quien hubiera presentado la factura sobre el estado de la misma. Además, la Ley 25/2013, de 27 de diciembre, otorga a la Intervención General de la Administración del Estado y a los órganos de control equivalentes en el ámbito autonómico y local la posibilidad de acceso al propio registro contable de facturas lo que les permitirá la elaboración de un informe anual sobre el cumplimiento de la normativa en materia de morosidad.

Esta Orden tiene carácter básico y es aplicable a todas las entidades incluidas en el ámbito de aplicación de la ley 25/2013, de 27 de diciembre, que deberán ajustar sus registros contables de facturas a las condiciones y requisitos funcionales y técnicos establecidos en esta Orden. Adicionalmente, se regulan las especialidades del registro contable de facturas de la Administración General del Estado y de cada una de las entidades públicas estatales de naturaleza administrativa.

La presente Orden regula los requisitos funcionales y técnicos del registro contable de facturas, con el fin de garantizar la integridad, seguridad e interoperabilidad de los distintos sistemas.

La Orden se estructura en tres capítulos, tres disposiciones adicionales y dos disposiciones finales, y va acompañada de un anexo.

El capítulo I «Disposiciones generales» describe el objeto de la norma, su ámbito de aplicación, el órgano competente para la gestión del registro contable de facturas y los objetivos de este registro.

El capítulo II «Requisitos funcionales» regula las anotaciones a practicar en el registro contable de facturas desde la recepción de éstas hasta el fin de su tramitación, así como el suministro de información a los proveedores sobre el estado de sus facturas.

El capítulo III «Requisitos técnicos» regula la interoperabilidad del registro contable de facturas con el Punto general de entrada de facturas electrónicas y la interoperabilidad a efectos de la distribución o puesta a disposición de los órganos competentes para su tramitación, así como la disponibilidad, confidencialidad, integridad y seguridad del propio registro.

La disposición adicional primera «Registro contable de facturas de la Administración General del Estado» incluye las especialidades funcionales y técnicas del registro contable de facturas en el ámbito estatal.

La disposición adicional segunda «No incremento de gasto público» dispone que las medidas contenidas en la Orden se atiendan con los medios personales y materiales existentes.

La disposición adicional tercera «Codificación de órganos administrativos» establece que las facturas que se expidan a partir de la entrada en vigor de esta Orden deberán ajustar su codificación de los órganos administrativos participantes en las mismas a la establecida en el directorio común DIR3 de unidades administrativas gestionado por la Secretaría de Estado de Administraciones Públicas.

La disposición final primera «Título competencial» declara el carácter básico de la Orden y recoge los preceptos constitucionales que le dan amparo.

La disposición final segunda «Entrada en vigor» dispone que la Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado», si bien las Comunidades Autónomas y Entidades Locales dispondrán de un periodo de tres meses para adecuar sus sistemas a los requisitos funcionales y técnicos establecidos en esta Orden.

El anexo recoge el contenido del fichero de datos personales «Registro contable de facturas de la AGE» creado en cumplimiento de lo dispuesto en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

Esta Orden se dicta en ejercicio de la habilitación legal otorgada al Ministro de Hacienda y Administraciones Públicas en la disposición final sexta y el artículo 9 de la Ley 25/2013, de 27 de diciembre y al amparo de los artículos 149.1.13ª, 149.1.14ª y 149.1.18ª de la Constitución Española.

En su virtud, de acuerdo con el Consejo de Estado, dispongo:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Orden tiene por objeto determinar los requisitos funcionales y técnicos del registro contable de facturas, con el fin de garantizar su integridad y seguridad, y la interoperabilidad con otros sistemas afectados en la tramitación de las facturas en desarrollo de la disposición final sexta de la Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el Sector Público.

Artículo 2. *Ámbito de aplicación.*

Esta Orden resulta de aplicación a los sujetos incluidos en el ámbito subjetivo establecido en el artículo 2 de la Ley 25/2013, de 27 de diciembre.

Las referencias hechas en esta Orden a las Administraciones Públicas se entenderán efectuadas a cada uno de los sujetos a que se refiere el párrafo anterior.

Artículo 3. *Órganos competentes en la gestión del sistema.*

El órgano competente para la gestión del registro contable de facturas será el órgano o unidad administrativa que tenga atribuida la función de contabilidad.

Artículo 4. *Objetivos del registro contable de facturas del sistema contable.*

1. El registro contable de facturas de cada Administración Pública estará interrelacionado o integrado en su sistema de información contable al objeto de registrar todas las facturas de la entidad con el alcance que se determina en la Ley 25/2013, de 27 de diciembre y de proporcionar al sistema contable la información necesaria para el seguimiento del cumplimiento de los compromisos de pago y para la determinación del periodo medio de pago a proveedores.

2. El registro contable de facturas de cada Administración Pública debe dar soporte a los siguientes requisitos funcionales:

a) Anotación inmediata en el correspondiente registro contable de facturas de las facturas recibidas en un registro administrativo con destino a una Administración Pública.

b) Distribución o puesta a disposición de las facturas anotadas en el registro contable de facturas de la entidad, a los órganos competentes para su tramitación.

c) Anotación en el registro contable de facturas de la aceptación o rechazo y devolución de las mismas por el órgano competente.

d) Anotación en el registro contable de facturas de la propuesta de anulación de la factura por el presentador de la misma y, en su caso, de su devolución por el órgano competente.

3. Sobre la base de la información gestionada en el registro contable de facturas y de la del sistema de información contable de la entidad:

a) La Administración Pública proporcionará información sobre el estado de las facturas a petición previa del proveedor o del presentador de las mismas, a través del registro administrativo de procedencia, entre ellos, en el caso de las facturas electrónicas, del que corresponda al respectivo Punto general de entrada de facturas electrónicas. No obstante,

en el caso de facturas en papel, cada entidad podrá establecer un procedimiento alternativo para proporcionar esta información.

b) Los órganos o unidades administrativas que tengan atribuida la función de contabilidad efectuarán requerimientos periódicos de actuación respecto a las facturas pendientes de reconocimiento de la obligación y demás actuaciones previstas en el artículo 10 de la Ley 25/2013, de 27 de diciembre.

CAPÍTULO II

Requisitos funcionales

Artículo 5. *Anotación en el registro contable de facturas.*

1. Las facturas recibidas por el registro administrativo serán anotadas en el registro contable de facturas, en los términos establecidos por la Ley 25/2013, de 27 de diciembre.

2. En el caso de las facturas electrónicas, se anotarán en el registro contable de facturas aquéllas que el Punto general de entrada de facturas electrónicas le remita o ponga a su disposición por medios electrónicos.

La información objeto de registro que debe ser remitida o puesta a disposición por el correspondiente Punto general de entrada de facturas electrónicas será, por cada factura, la propia factura electrónica, el número de asiento registral asignado en el registro asociado al mencionado Punto, y la fecha y hora de dicho asiento registral.

3. En el caso de las facturas en papel, se generará un apunte en el registro contable de facturas, por cada factura recibida, incluyendo al menos la siguiente información:

a) Fecha de expedición de la factura.

b) Fecha de presentación de la factura en el registro administrativo.

c) Número de Identificación Fiscal o número de identificación equivalente del expedidor de la factura.

d) Nombre y apellidos, razón o denominación social completa del obligado a expedir factura.

e) Número de factura y, en su caso, serie.

f) Importe de la operación, incluido IVA (o impuesto equivalente).

g) Unidad monetaria en la que está expresado el importe, de acuerdo con la codificación ISO 4217 Alpha-3.

h) Código de los órganos competentes en la tramitación de la factura así como del órgano o unidad administrativa que tenga atribuida la función de contabilidad, codificado de acuerdo con el directorio DIR3 de unidades administrativas gestionado por la Secretaría de Estado de Administraciones Públicas.

4. No se anotarán en el registro contable de facturas las que contuvieran datos incorrectos u omisión de datos que impidieran su tramitación, ni las que correspondan a otras Administraciones Públicas, las cuales serán devueltas al registro administrativo de procedencia con expresión de la causa de dicho rechazo.

Artículo 6. *Distribución o puesta a disposición de las facturas anotadas en el registro contable de facturas de la entidad.*

1. Las facturas anotadas en el registro contable de facturas serán distribuidas o puestas a disposición de los correspondientes órganos competentes para su tramitación, de acuerdo con la identificación de esos órganos o unidades que figure en la propia factura, a efectos de tramitar, si procede, el procedimiento de conformidad con la entrega del bien o la prestación del servicio realizada por quien expidió la factura y proceder al resto de actuaciones relativas al expediente de reconocimiento de la obligación, incluida, en su caso, la remisión al órgano de control competente a efectos de la preceptiva intervención previa.

2. En el caso de las facturas electrónicas, serán remitidas o puestas a disposición de los correspondientes órganos competentes para su tramitación, por los medios electrónicos que se habiliten, aquellas facturas anotadas en el registro contable de facturas que les correspondan.

Artículo 7. *Anotación en el registro contable de facturas de la aceptación o rechazo de las mismas.*

La aceptación o rechazo de cada factura se anotará en el registro contable de facturas, dejando constancia de la fecha en que se haya producido. Asimismo se anotará en el registro contable de facturas, en caso de aprobación de la conformidad y reconocimiento de la obligación, la fecha de contabilización de la obligación reconocida correspondiente. No obstante, si con respecto a cualquier factura se contabilizase una obligación por operaciones pendientes de aplicar al presupuesto, igualmente se anotará la fecha de dicha contabilización en el indicado registro.

Por cada factura se dejará constancia en el sistema de información contable de la fecha en la que se inicia el cómputo del plazo de pago según establece el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.

Artículo 8. *Anotación en el registro contable de facturas de la propuesta de anulación de la factura y de su devolución.*

1. Cuando en el registro contable de facturas se reciba, a través del registro administrativo o, en el caso de las facturas electrónicas, el que corresponda al respectivo Punto general de entrada de facturas electrónicas, una solicitud del presentador de anulación de una factura anterior, se tomará nota de la solicitud de anulación en el registro contable de facturas, cuando esa factura ya estuviera anotada en dicho registro. En caso contrario, será rechazada y devuelta la solicitud al registro administrativo que la remitió.

2. Las solicitudes de anulación de las que se hubiera tomado nota en el registro contable de facturas serán comunicadas a los correspondientes órganos competentes para su tramitación, a efectos de que procedan a su estimación y subsiguiente devolución de la factura, previa anulación, si fuera el caso, de las anotaciones que se hubieran efectuado en dicho registro en relación con la factura, o a su rechazo.

Artículo 9. *Suministro de información sobre el estado de las facturas.*

1. Sobre la base de la información del registro contable de facturas, la Administración Pública proporcionará información sobre el estado de las facturas a petición previa del proveedor o del presentador de las mismas, a través del registro administrativo de procedencia, entre ellos, en el caso de las facturas electrónicas, del que corresponda al respectivo Punto general de entrada de facturas electrónicas. No obstante, en el caso de facturas en papel, cada Administración podrá establecer un procedimiento alternativo para proporcionar esta información.

2. El proveedor tendrá derecho a conocer los siguientes estados de la factura: si ha sido registrada en el registro contable de facturas; si ha sido contabilizada la obligación reconocida; si ha sido pagada; anulada; y rechazada.

CAPÍTULO III

Requisitos técnicos

Artículo 10. *Interoperabilidad del registro contable de facturas con el Punto general de entrada de facturas electrónicas.*

1. La determinación de las condiciones técnicas normalizadas de las interfaces entre el Punto general de entrada de facturas electrónicas adoptado por cada Administración y el registro contable de facturas de las Administraciones Públicas corresponderá, conjuntamente, a la Secretaría de Estado de Administraciones Públicas y a la Intervención General de la Administración del Estado, oído el Consejo Superior de Administración Electrónica.

2. La anotación en el registro contable de facturas de las facturas electrónicas procedentes del correspondiente Punto general de entrada de facturas electrónicas, a la que se refiere el artículo 5.2, se efectuará utilizando los servicios de puesta electrónica a

disposición que proporcione el propio Punto, que se ajustarán a las condiciones técnicas normalizadas a las que se refiere el apartado anterior.

Artículo 11. *Interoperabilidad del registro contable de facturas a efectos de la distribución o puesta de las facturas a disposición de los órganos competentes para su tramitación.*

1. La distribución o puesta a disposición de las facturas electrónicas anotadas en el registro contable de facturas a los correspondientes órganos competentes para su tramitación, a la que se refiere el artículo 6.2, se efectuará utilizando los servicios o medios electrónicos que al efecto habilite la entidad.

2. Los órganos competentes para su tramitación deberán disponer de sistemas o medios para la tramitación de aquellos expedientes de gasto que incorporen facturas electrónicas.

Artículo 12. *Disponibilidad, confidencialidad, integridad y seguridad del registro contable de facturas.*

1. El sistema contará con medidas de redundancia, proporcionales a los riesgos asumidos, que permitan minimizar los períodos de fallo.

La disponibilidad horaria del sistema estará publicada en el portal o sede electrónica que corresponda al órgano o unidad administrativa que tenga atribuida la función de contabilidad.

2. A los datos de carácter personal contenidos en este sistema se aplicarán las medidas de seguridad del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

3. Las medidas de seguridad y salvaguardia de la información se ajustarán a lo establecido en la política de seguridad del órgano o unidad administrativa que tenga atribuida la función de contabilidad.

4. La acreditación de los usuarios que accedan al registro contable de facturas, tanto los del órgano o unidad administrativa que tenga atribuida la función de contabilidad como los de los órganos competentes para su tramitación, deberá efectuarse de acuerdo con los procedimientos que al efecto establezca el órgano o unidad administrativa que tenga atribuida la función de contabilidad.

Los usuarios de los órganos competentes para la tramitación de las facturas sólo podrán acceder a aquéllas que tuvieran asignadas.

Cuando el registro contable de facturas haga uso de los servicios o medios de interoperabilidad señalados en el artículo 11 de esta Orden, la acreditación de los sistemas con los que se relacione el registro contable de facturas deberá efectuarse de acuerdo con los procedimientos que al efecto establezca el órgano o unidad administrativa que tenga atribuida la función de contabilidad.

5. El sistema se ajustará a lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Disposición adicional primera. *Registro contable de facturas de la Administración General del Estado.*

El registro contable de facturas de la Administración General del Estado y el correspondiente a cada una de las entidades públicas estatales de naturaleza administrativa se ajustará a las condiciones y requisitos funcionales y técnicos establecidos en esta Orden con las siguientes particularidades:

1. Aspectos organizativos:

a) La Intervención General de la Administración del Estado será el órgano competente para:

1.º La gestión, administración y mantenimiento del registro contable de facturas de la Administración General del Estado.

2.º La definición de las especificaciones del sistema.

3.º La determinación de las condiciones técnicas normalizadas de las interfaces del registro contable de facturas con los sistemas de gestión económico-presupuestaria de las unidades tramitadoras competentes para la tramitación de las facturas electrónicas.

b) La gestión, administración y mantenimiento del registro contable de facturas de cada una de las entidades públicas estatales de naturaleza administrativa será el centro directivo u órgano gestor de la contabilidad de la entidad.

c) La gestión y actualización del catálogo de órganos gestores y unidades tramitadoras, y del responsable de fichero y usuario administrador de cada unidad tramitadora, en el propio sistema de información contable, será efectuada por la correspondiente oficina contable.

d) Las unidades tramitadoras y los órganos de control establecerán en sus respectivos sistemas de gestión, si fuera necesario, la correspondencia entre las codificaciones establecidas para los órganos gestores y unidades tramitadoras en el registro contable de facturas, basada en el directorio DIR3 de unidades administrativas de la Secretaría de Estado de Administraciones Públicas, y las utilizadas en sus respectivos sistemas.

e) La gestión de los usuarios de las unidades tramitadoras con acceso permitido al correspondiente registro contable de facturas, y de los correspondientes perfiles de acceso, corresponderá al usuario administrador designado por cada unidad tramitadora. Asimismo este usuario administrador gestionará en el propio sistema de información contable la asignación de órganos gestores a los que dará servicio a estos efectos.

f) Cuando la acreditación de acceso al sistema por parte de un usuario, directamente, o de un órgano gestor o unidad tramitadora, a través de su correspondiente sistema de gestión, requiera un certificado electrónico, deberá estar expedido por un prestador de servicios de certificación que figure en la lista de servicios de confianza (TSL) publicada por el Ministerio de Industria, Energía y Turismo, y estar asumido por la plataforma de verificación de certificados, de la Secretaría de Estado de Administraciones Públicas, prevista en el artículo 21.3 de la Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos.

g) Cuando se produzcan cambios estructurales o reorganizaciones administrativas que provoquen cambios en las codificaciones de las oficinas contables, órganos gestores y unidades tramitadoras se estará a lo que establezca al efecto la Intervención General de la Administración del Estado.

2. Anotación de las facturas por la oficina contable.

Las facturas, tanto electrónicas como en papel, recibidas por la oficina contable, antes de su distribución o puesta a disposición de las unidades tramitadoras, serán objeto de anotación por la oficina contable en el registro contable de facturas. Si detectara datos incorrectos u omisión de datos que impidieran su distribución, o que las facturas no le correspondieran por tratarse de facturas de otra Administración Pública, las rechazará, devolviéndolas al registro administrativo de procedencia con expresión de la causa de dicho rechazo.

3. Distribución de las facturas anotadas en el registro contable de facturas.

Por cada factura la oficina contable remitirá o pondrá a disposición de la unidad tramitadora la propia factura electrónica, y el código, fecha y hora de anotación en el registro contable de facturas, debiendo quedar constancia en el mismo de la fecha y hora de recepción o descarga por la unidad tramitadora.

En el caso de las facturas en papel, se remitirán a cada unidad tramitadora las facturas anotadas en el registro contable de facturas que le correspondan. La oficina contable dejará constancia en el registro contable de facturas de la fecha del acuse de recibo por la unidad tramitadora.

4. Anotación en el registro contable de facturas de la aceptación o rechazo y devolución de las mismas por el órgano gestor.

a) Cuando proceda la aceptación de la factura, la unidad tramitadora anotará en el registro contable de facturas, por los medios electrónicos que al efecto habilite la oficina contable, la aceptación de la factura, dejando constancia de la fecha en la que se ha producido dicha aceptación.

b) Asimismo, cuando no proceda la aceptación de la factura, la unidad tramitadora anotará en el registro contable de facturas, por los medios electrónicos que al efecto habilite la oficina contable, el rechazo de la factura y su devolución a través de la oficina contable, dejando constancia de la fecha en la que se ha producido dicho rechazo.

5. Anotación en el registro contable de facturas en relación con el reconocimiento de la obligación y el pago de las mismas.

a) Para aquellas facturas de pago directo a las que se haya prestado la correspondiente aprobación de la conformidad y reconocimiento de la obligación, se dejará constancia en el propio registro contable de facturas, preferentemente de forma automática, del número de operación contable que se hubiera registrado en el respectivo sistema de información contable como consecuencia de la obligación reconocida, y de las fechas de dicha obligación y del pago posterior, a efectos de lo cual tanto la anotación de obligación reconocida como la del pago material identificarán la factura o facturas asociadas mediante los correspondientes códigos de registro contable de facturas.

b) Cuando las facturas se tramiten como anticipos de caja fija o pagos a justificar la unidad tramitadora anotará en el propio registro contable de facturas, para cada factura, por los medios electrónicos que se habiliten, en su caso el número de libramiento de pagos a justificar, y la fecha de pago de la factura.

6. De acuerdo con lo previsto en el tercer párrafo del artículo 9.1 de la Ley 25/2013, de 27 de diciembre, se excluye de la obligación de anotación en el registro contable de facturas de la Administración General del Estado y de las entidades públicas estatales de naturaleza administrativa:

a) A las facturas en papel cuyo importe sea de hasta 5.000 euros.

b) A las facturas, electrónicas y en papel, emitidas por los proveedores a los servicios en el exterior hasta que se haya consolidado el uso de la factura electrónica y se disponga de los medios y sistemas apropiados para su recepción en dichos servicios.

7. Fichero de Protección de Datos.

En cumplimiento de lo previsto en el artículo 20 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se crea el fichero de datos personales, «Registro Contable de Facturas de la AGE», cuya titularidad corresponde a la Intervención General de la Administración del Estado, válido a efectos del ejercicio por parte de los ciudadanos de los derechos previstos por dicha ley. El contenido del fichero se recoge en el anexo I de la presente Orden.

Disposición adicional segunda. *No incremento de gasto público.*

Las medidas contenidas en esta Orden se atenderán con los medios personales y materiales existentes, y en ningún caso podrá generar incremento de gasto público.

Disposición adicional tercera. *Codificación de órganos administrativos.*

Las facturas que se expidan a partir de la entrada en vigor de esta Orden ajustarán la codificación de los órganos administrativos que participen en la tramitación de las mismas a la establecida en el directorio DIR3 de unidades administrativas comunes gestionado por la Secretaría de Estado de Administraciones Públicas.

Disposición adicional cuarta. *Reglas de validación de las facturas electrónicas aplicables en fase de anotación en los registros contables de facturas.*

1. Los sistemas de información contable en los que estén integrados los registros contables de facturas de las entidades sujetas al ámbito de aplicación de la Ley 25/2013, de 27 de diciembre, ajustarán sus reglas de validación en fase de anotación de dichas facturas en el registro contable de facturas, antes de 15 de octubre de 2015, a las contenidas en el anexo II de esta Orden.

Estas reglas de validación serán las aplicables por todos los registros contables de facturas a efectos de la anotación de las facturas electrónicas recibidas del punto general de entrada de facturas electrónicas en dichos registros, de forma que solamente aquéllas que

no superen las validaciones establecidas en dicho anexo podrán ser rechazadas en esta fase. El resto de facturas quedarán anotadas automáticamente en el registro contable de facturas, disponibles para su tramitación posterior, sin que ello prejuzgue el resultado de la misma.

En todo caso el rechazo de una factura, cualquiera que sea la fase en que se produzca, requerirá la cumplimentación del motivo del rechazo por parte de la Administración.

2. Las reglas de validación vigentes serán publicadas en el Portal web de la Intervención General de la Administración del Estado, en el apartado destinado al registro contable de facturas, y en el Portal web del Punto General de Entrada de facturas electrónicas de la Administración General del Estado (FACe).

3. El Ministerio de Hacienda y Administraciones Públicas publicará en los Portales indicados en el punto anterior una utilidad para la verificación de las reglas de validación de la factura electrónica vigentes que no dependan de la información del registro contable de facturas. Esta utilidad dará soporte asimismo a la validación de cualquier extensión aprobada por el Ministerio.

Disposición final primera. *Título competencial.*

Excepto en lo que se refiere a la disposición adicional primera, el contenido de esta Orden tiene carácter básico y se dicta al amparo de lo dispuesto en los apartados 13, 14 y 18 del artículo 149.1 de la Constitución Española que atribuyen al Estado, respectivamente, la competencia sobre las bases y coordinación de la planificación general de la actividad económica; Hacienda general y Deuda del Estado y las bases del régimen jurídico de las Administraciones públicas.

Disposición final primera bis. *Habilitación normativa.*

Se habilita a los titulares de las Secretarías de Estado de Presupuestos y Gastos y de Hacienda, en el ámbito de sus competencias, a adoptar las resoluciones y medidas necesarias para la aplicación y ejecución de lo dispuesto en esta Orden.

En particular, el contenido del anexo II de esta Orden podrá ser modificado por resolución conjunta del titular de la Secretaría de Estado de Presupuestos y Gastos y del titular de la Secretaría de Estado Hacienda, oído el Comité Sectorial de Administración Electrónica.

Disposición final segunda. *Entrada en vigor.*

La presente Orden entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

No obstante lo anterior, las Comunidades Autónomas y Entidades locales dispondrán de un periodo de 3 meses para adecuar sus sistemas a los requisitos funcionales y técnicos establecidos en esta orden.

ANEXO I

Fichero de datos de carácter personal

Nombre del fichero: «Registro contable de facturas de la AGE»

Finalidad del fichero y usos previstos: anotación de las facturas recibidas en la Administración General del Estado, bien mediante recepción automática desde el servicio FACe – Punto general de entrada de facturas electrónicas de la Administración General del Estado, o por captura de determinados datos de la factura en papel; validación por la oficina contable de las facturas recibidas; distribución de las mismas a los órganos gestores a través de sus unidades tramitadoras, a efectos de tramitar, si procede, el procedimiento de conformidad con la entrega del bien o la prestación del servicio realizada por quien expidió la factura y proceder al resto de actuaciones relativas al expediente de reconocimiento de la obligación; y control de la morosidad en el pago de las facturas.

Personas o colectivos sobre los que se pretende obtener datos de carácter personal, o que resulten obligados a suministrarlos: terceros de las facturas que sean remitidas a los órganos gestores de la Administración General del Estado.

Procedimiento de recogida de datos de carácter personal: De los datos del tercero en la propia factura recibida en la Administración General del Estado.

Estructura básica del fichero y descripción de los tipos de datos de carácter personal, incluidos en el mismo: Se recogerán los siguientes datos personales:

Datos del emisor/proveedor:

Código de identificación fiscal.
Nombre y apellidos.
Dirección.

Datos del cesionario (si lo hubiera):

Código de identificación fiscal.
Nombre y apellidos.
Dirección.

Datos del emisor/tercera persona (si lo hubiera):

Código de identificación fiscal.
Nombre y apellidos.
Dirección.

Datos de persona de contacto:

Nombre y apellidos.
Teléfono.
Fax.
Correo electrónico.
URL.

Datos de pago:

Cuenta de abono.

Sistema de tratamiento: Fichero automatizado.

Comunicaciones previstas de los datos, indicando, en su caso, los destinatarios o categorías de destinatarios: Comunicación de datos a los Órganos gestores de las Administraciones Públicas en las que se han creado los registros contables de facturas a efectos de la conformidad de las mismas y tramitación de los expedientes de reconocimiento de la obligación, comunicación periódica de datos a la Agencia Estatal de Administración Tributaria para la verificación del cumplimiento de las obligaciones tributarias y de facturación, y comunicación de datos al Tribunal de Cuentas y Órganos de Control Externo de las Comunidades Autónomas, a solicitud de dichos órganos, a efectos del desarrollo de sus funciones como superiores órganos fiscalizadores de las Administraciones Públicas.

Transferencias internacionales previstas a terceros países, con indicación, en su caso, de los países de destino de los datos: No previstas.

Órganos responsables del fichero: Subdirección General de Gestión Contable de la Intervención General de la Administración del Estado del Ministerio de Hacienda y Administraciones Públicas.

Servicios o unidades ante los que pueden ejercitarse los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Gestión Contable de la Intervención General de la Administración del Estado del Ministerio de Hacienda y Administraciones Públicas, calle María de Molina, número 50, 28071, Madrid.

Nivel básico, medio o alto de seguridad: Nivel básico.

ANEXO II

Reglas de validación a las que se refiere la disposición adicional cuarta

1. Verificación del cumplimiento del esquema XSD de "Facturae" de la versión correspondiente (3.2 ó 3.2.1), así como verificación de los XSD de las extensiones aprobadas.

2. Verificación de la política de firma en vigor asociada al formato "Facturae".

3. Respecto al número de la factura:

a) El número de factura será obligatorio.

b) No deberá existir en el registro contable de facturas una factura con el mismo NIF y país del emisor, número y serie de factura, emitida en la misma fecha, salvo que estuviera rechazada o anulada.

4. Respecto al tipo de factura electrónica.

a) La tipología de facturas rectificativas admitidas en el formato Facturae, de acuerdo con el Real Decreto 1619/2012, de 30 de noviembre, por el que se aprueba el Reglamento por el que se regulan las obligaciones de facturación, será la siguiente:

1.º "01" - Rectificación modelo íntegro.

2.º "02" - Rectificación modelo por diferencias.

3.º "03" - Rectificación por descuento por volumen de operaciones durante un período y rectificación por devolución de mercancías o de envases y embalajes previstos en el artículo 15.2, 2.º párrafo, del Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre.

4.º "04" - Autorizadas por la Agencia Estatal de Administración Tributaria.

b) Cuando el tipo de factura es rectificativa, será obligatorio el criterio de rectificación y, cuando este criterio fuera 01, rectificación modelo íntegro, o 02, rectificación modelo por diferencias, el número de factura del emisor que rectifica. En el resto de supuestos no será necesario identificar el número de factura del emisor que rectifica.

c) Si en el registro contable de facturas ha sido ya registrada la factura original, debería rechazarse el duplicado o copia de la misma previsto en el artículo 14 del Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre. En el caso de que la factura original llegara al registro contable de facturas una vez registrado el duplicado o copia, se rechazaría aquélla.

5. Respecto al emisor y cesionario de la factura.

a) El código de tipo de persona, física o jurídica, será obligatorio. En el caso de entidades sin personalidad jurídica se utilizará el código correspondiente a personas jurídicas.

b) En el caso de que el país emisor del NIF sea España, se validará que el NIF se ajuste a las normas y criterios de formación del mismo. Si los dos primeros caracteres del NIF son letras, se asumirá que equivalen al país, y el resto al NIF. En otro caso, el código equivaldrá al NIF y se asumirá que el país es España.

c) Se validará la existencia del código del país de acuerdo con el propio esquema "Facturae".

d) Si se trata de persona física, se validará que el nombre y el primer apellido tengan algún contenido.

e) Si se trata de persona jurídica, se validará que la razón social tenga algún contenido.

f) Si existe cesionario, se comprobará que el NIF del emisor de la factura y del cesionario no coinciden.

6. Respecto a los importes de la factura.

a) En las facturas emitidas en euros, se validará que los importes totales de las líneas relativos al coste total sean numéricos y estén redondeados, de acuerdo con el método común de redondeo, a dos decimales, como resultado del producto del número de unidades por el precio unitario, y que los importes brutos de las líneas sean el resultado de restar del coste total los descuentos, y de sumar los cargos, todos ellos numéricos y con dos

decimales. Asimismo se validará que el resto de importes a nivel de línea, con excepción del importe unitario, vengan expresados en euros con dos decimales. No se consideran importes los tipos impositivos o los porcentajes a aplicar que, al igual que el importe unitario, podrán tener los decimales que permita el formato Facturae.

b) En las facturas emitidas en euros, se validará que el total importe bruto de la factura sea numérico y a dos decimales, por suma de los importes brutos de las líneas. Asimismo se validará que el resto de importes vengan expresados en euros con dos decimales. No se consideran importes los tipos impositivos o los porcentajes a aplicar que podrán tener los decimales que permita el formato Facturae.

c) Se validará la existencia del código de moneda de acuerdo con lo establecido en el propio esquema "Facturae".

d) Si el "total importe bruto antes de impuestos" es positivo, se validará que el "total impuestos retenidos", si tiene contenido, sea mayor o igual que cero.

e) Se validará que el "total importe bruto antes de impuestos" sea igual al "total importe bruto" menos el "total general descuentos" más el "total general cargos".

f) Se validará que el "total Factura" sea igual al "total importe bruto antes de impuestos" más el "total impuestos repercutidos" menos el "total impuestos retenidos".

7. Respecto a las fechas de la factura.

a) Se validará que la fecha de anotación en el registro administrativo tenga valor, sea válida y anterior o igual a la fecha actual y mayor o igual que la fecha de emisión de la factura.

8. Respecto a los órganos administrativos que participan en la tramitación de la factura.

a) Se validará que los códigos DIR3 de los tres órganos administrativos que resulta obligatorio identificar en la factura electrónica tengan valor y existan en las tablas de órganos administrativos del registro contable de facturas.

b) Se validará que las relaciones oficina contable-órgano gestor; oficina contable-unidad tramitadora; y órgano gestor-unidad tramitadora existan en las tablas de órganos administrativos del registro contable de facturas.

9. Otras validaciones.

a) Será obligatorio que el punto general de entrada de facturas electrónicas proporcione, por cada factura electrónica presentada, el número de registro asignado en dicho punto.

b) Se validará que la descripción de las líneas de la factura tenga algún contenido.

§ 52

Orden PRE/2794/2011, de 5 de octubre, por la que se publica el Acuerdo del Consejo de Ministros, de 19 de agosto de 2011, por el que se determina el marco de ejercicio de las competencias estatales en materia de factura electrónica, se crea el Foro Nacional Multilateral sobre facturación electrónica y se impulsa el Servicio Central de Gestión de la Facturación Electrónica en el ámbito de la Administración General del Estado

Ministerio de la Presidencia
«BOE» núm. 251, de 18 de octubre de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-16400

El Consejo de Ministros, en su reunión del día 19 de agosto de 2011 y a propuesta del Ministro de Industria, Turismo y Comercio, de la Vicepresidenta del Gobierno para Asuntos Económicos y Ministra de Economía y Hacienda y del Vicepresidente del Gobierno para Política Territorial y Ministro de Política Territorial y Administración Pública, ha adoptado un Acuerdo por el que se determina el marco de ejercicio de las competencias estatales en materia de factura electrónica, se crea el Foro Nacional Multilateral sobre facturación electrónica y se impulsa el Servicio Central de Gestión de la Facturación Electrónica en el ámbito de la Administración General del Estado.

Para general conocimiento se dispone su publicación como anexo a la presente orden.

ANEXO

Acuerdo por el que se determina el marco de ejercicio de las competencias estatales en materia de factura electrónica, se crea el Foro Nacional Multilateral sobre facturación electrónica y se impulsa el Servicio Central de Gestión de la Facturación Electrónica en el ámbito de la Administración General del Estado

La estrategia «Europa 2020», de la Comisión Europea, incluye entre sus prioridades el desarrollo de una economía basada en el conocimiento y la innovación, que haga un uso más eficaz de los recursos, siendo la digitalización y automatización de procesos administrativos un factor clave en la mejora de la productividad de las economías. En ese sentido, las medidas para avanzar en la penetración de la facturación electrónica permiten dar un paso esencial para construir un mercado único digital en Europa, permitiendo la superación de obstáculos de carácter regulador y tecnológico. La Comisión Europea ha incluido la facturación electrónica como parte de la «Agenda Digital para Europa», al considerar que su uso generalizado permite la obtención de ganancias significativas en los

entornos de contratación, pagos, tributación, procesos contables y auditoría, y se configura como soporte para consolidar el comercio electrónico.

La factura electrónica es un documento electrónico que cumple con los requisitos legal y reglamentariamente exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor.

El establecimiento de requisitos de seguridad para la facturación electrónica se realizó mediante el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el Reglamento que regula las obligaciones de facturación y se modifica el Reglamento del IVA, que establece que las facturas electrónicas deberán incorporar medios que garanticen la autenticidad del origen y la integridad de su contenido. Estos requisitos fueron detallados en la Orden EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas contenidas en el anterior Real Decreto.

Asimismo, la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información prevé en su texto un plan para la generalización del uso de la factura electrónica y establece que el Gobierno determinará el órgano competente de la Administración General del Estado que impulsará el empleo de la factura electrónica entre empresarios, profesionales y demás agentes del mercado, en particular, entre las pequeñas y medianas empresas y en las denominadas microempresas, con el fin de fomentar el desarrollo del comercio electrónico.

Por su parte, el Gobierno, en el diseño de los Planes Avanza y Avanza 2 ha incorporado el citado plan de generalización del uso de la factura electrónica previsto en la Ley de Medidas de Impulso de la Sociedad de la Información. De manera particular, la Estrategia 2011-2015 del Plan Avanza 2 contempla la difusión del uso de la facturación electrónica en su objetivo 7: «Extender el uso de soluciones TIC (Tecnologías de la Información y las Comunicaciones) de negocio en la empresa».

El plan de generalización del uso de la factura electrónica incardinado en el Plan Avanza se ha elaborado previa amplia consulta pública realizada a las asociaciones relevantes representativas de las entidades proveedoras de soluciones técnicas de facturación electrónica, a las asociaciones relevantes de usuarios de las mismas y a los colegios profesionales que agrupan a técnicos del sector de la Sociedad de la Información y de las Telecomunicaciones. Las líneas estratégicas de actuación definidas en el plan son: la comunicación y formación sobre la factura electrónica, la difusión de herramientas para la gestión de la factura electrónica, el desarrollo de servicios de factura electrónica, las ayudas para la incorporación de la factura electrónica, el fomento de la confianza en la factura electrónica, la accesibilidad en la visualización de la factura electrónica y el mantenimiento y evolución del formato de factura electrónica facturae.

Asimismo, y a efectos de mejorar la eficiencia en la Administración, mediante este Acuerdo se da un mandato al Ministerio de Política Territorial y Administración Pública para que lidere la definición y desarrollo en 2011 de un servicio central de gestión de la facturación electrónica para el ámbito de la Administración General del Estado. Este servicio de gestión será el medio único para la recepción y distribución de facturas electrónicas, salvo excepciones claras y debidamente justificadas que deberán ser aprobadas en la Comisión Permanente del Consejo Superior de Administración Electrónica. Asimismo, este servicio podrá proporcionar funcionalidades de almacenamiento y custodia de las facturas electrónicas.

Por otra parte, la Comunicación de la Comisión Europea COM (2010) 712, de 2 de diciembre de 2010, «Aprovechar en Europa las ventajas de la facturación electrónica», con el objetivo de que la facturación electrónica sea el método prevalente de facturación en Europa a más tardar en 2020, establece las siguientes prioridades: garantizar la seguridad jurídica y condiciones técnicas claras para la facturación electrónica; alentar y favorecer el desarrollo de soluciones de facturación electrónica abiertas e interoperables basadas en una norma técnica común, prestando especial atención a las necesidades de la Pyme; y respaldar el uso de la facturación electrónica mediante el establecimiento de estructuras organizativas. Entre estas últimas, se insta a la creación por parte de cada Estado Miembro de un Foro Nacional Multilateral sobre facturación electrónica.

La Comunicación de la Comisión Europea cita que en este Foro Nacional Multilateral habrán de estar representados, de manera equilibrada, los diferentes agentes implicados en el desarrollo de la factura electrónica, con una participación suficiente de las autoridades públicas y los usuarios de los servicios de facturación electrónica, incluyendo consumidores, pequeñas y medianas empresas, y grandes empresas.

En respuesta a la petición de la Comisión Europea, el presente Acuerdo crea el Foro Nacional Multilateral sobre facturación electrónica en España (Foro Nacional).

En este marco, y para propiciar un apoyo decisivo a la implantación de la factura electrónica, la Comisión Europea ha acordado, mediante Decisión C (2010) 8467, de 2 de diciembre, la constitución del Foro Europeo Multilateral sobre facturación electrónica (Foro Europeo), para facilitar el intercambio de experiencias y buenas prácticas y para asistir a la Comisión en la identificación de medidas que faciliten la adopción y generalización del uso de la factura electrónica en todos los Estados miembros. El Foro Europeo estará compuesto por representantes de los Foros Nacionales y de asociaciones europeas vinculadas al desarrollo e implantación de la factura electrónica, así como por otras organizaciones y grupos de trabajo, entre los que figurarán el Banco Central Europeo, el Comité Europeo para la Normalización y el Grupo de Trabajo del artículo 29 sobre Protección de Datos. Cada Estado miembro habrá de proponer dos candidatos que representen a sus Foros Nacionales en las reuniones del Foro Europeo. El presente Acuerdo determina el mecanismo para la designación de los representantes españoles en el Foro Europeo.

En su virtud, a propuesta conjunta del Ministro de Industria, Turismo y Comercio, de la Vicepresidenta del Gobierno para Asuntos Económicos y Ministra de Economía y Hacienda y del Vicepresidente del Gobierno para Política Territorial y Ministro de Política Territorial y Administración Pública, el Consejo de Ministros, en su reunión del día 19 de agosto de 2011, acuerda:

Determinar el marco de ejercicio de las competencias estatales en materia de facturación electrónica, aprobar determinadas medidas en materia de difusión del uso de la factura electrónica y la creación de un Foro Nacional Multilateral sobre facturación electrónica.

Para ello, se adoptan las siguientes medidas:

1. El Ministerio de Industria, Turismo y Comercio será el órgano de la Administración General del Estado que ejercerá las competencias estatales en materia de difusión del uso de la factura electrónica en España en el sector privado, en particular, en las Pymes.

2. El Ministerio de Política Territorial y Administración Pública será el órgano de la Administración General del Estado que ejercerá las competencias en materia de difusión del uso de la factura electrónica en la Administración General del Estado.

3. Se crea, al amparo de lo dispuesto en el artículo 40.3 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, la Comisión Técnica para la difusión del uso de la factura electrónica, de carácter consultivo, con el objetivo de asistir a los Ministerios de Industria, Turismo y Comercio y de Política Territorial y Administración Pública en el desarrollo de las competencias señaladas en los apartados 1 y 2.

4. La Comisión Técnica estará constituida por un representante designado por cada uno de los departamentos siguientes: Ministerio de Industria, Turismo y Comercio, Ministerio de Política Territorial y Administración Pública y Ministerio de Economía y Hacienda. Su Presidente será designado por el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información. En casos de vacante, ausencia, enfermedad u otra causa legal, el Presidente será sustituido por el representante del Ministerio de Industria, Turismo y Comercio. Los miembros de la Comisión Técnica formarán parte del Foro Nacional al que se refiere el apartado 5. Actuará como Secretario un funcionario de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información designado por el Presidente.

5. Se crea, al amparo de lo dispuesto en el artículo 40.3 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, el Foro Nacional Multilateral sobre facturación electrónica (en adelante, Foro Nacional), que tendrá un carácter consultivo en materia de facturación electrónica. Este Foro estará presidido por el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información. En

casos de vacante, ausencia, enfermedad u otra causa legal, el Presidente será sustituido por el Presidente de la Comisión Técnica referida en el apartado 4.

6. El Foro Nacional se compondrá de los miembros de la Comisión Técnica regulada en los puntos 3 y 4, así como de un representante por cada una de las siguientes entidades designado por el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información a propuesta de las entidades correspondientes:

a) Asociación de Multisectorial de Empresas de la Electrónica, las Tecnologías de la Información y la Comunicación, de las Telecomunicaciones y de los Contenidos Digitales (AMETIC).
b) Asociación Nacional de Empresas de Internet (ANEI).
c) Asociación Española de Usuarios de Telecomunicaciones y de la Sociedad de la Información (AUTELSI).
d) Asociación Española de la Economía Digital (ADIGITAL).
e) Consejo de Consumidores y Usuarios (CCU).
f) Centro de Cooperación Interbancario (CCI).
g) Confederación Española de Organizaciones Empresariales (CEOE).

Asimismo, podrán participar en el Foro Nacional los representantes en la Comisión Permanente del Consejo Asesor de Telecomunicaciones y para la Sociedad de la Información de las Comunidades Autónomas y de la Federación Española de Municipios y Provincias.

El Presidente del Foro Nacional podrá invitar a las reuniones y trabajos del mismo a los expertos en la materia que estime pertinentes.

Actuará como Secretario un funcionario de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información designado por el Presidente.

7. La actividad del Foro Nacional se desarrollará en los siguientes ámbitos:

a) Proponer iniciativas para promover la adopción de la factura electrónica en España, en ámbitos tales como el normativo o la estandarización e interoperabilidad.
b) Asesorar en la elaboración y puesta en marcha de actuaciones para la difusión del uso de la factura electrónica en España.
c) Colaborar en las acciones para difundir el uso de la factura electrónica en España, en particular, en el ámbito de las Pymes.
d) Facilitar el intercambio de experiencias y buenas prácticas en el proceso de desarrollo e implantación de la factura electrónica en España.
e) Realizar, en su caso, análisis y estudios sobre la adopción de la factura electrónica en los diferentes sectores económicos.

8. El Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información designará a dos representantes en el Foro Europeo constituido mediante la Decisión de la Comisión, de 2 de diciembre de 2010, por la que se establece un Foro Multilateral Europeo sobre Facturación Electrónica.

9. El Ministerio de Política Territorial y Administración Pública, a través de la Secretaría de Estado para la Función Pública, liderará la definición y desarrollo en 2011 de un servicio central de gestión de la facturación electrónica para el ámbito de los órganos de la Administración General del Estado, sus organismos autónomos y agencias estatales definidas en la Ley 28/2006, de 18 de julio, de agencias estatales para la mejora de los servicios públicos. Este servicio de gestión será el medio único para la recepción y distribución de facturas electrónicas, salvo excepciones claras y debidamente justificadas, que deberán ser aprobadas en la Comisión Permanente del Consejo Superior de Administración Electrónica. Asimismo, este servicio podrá proporcionar funcionalidades de almacenamiento y custodia de las facturas electrónicas.

10. El Ministerio de Industria, Turismo y Comercio, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, continuará impulsando en 2011 el uso de la factura electrónica con actuaciones de información destinadas a ciudadanos y la generación de contenidos didácticos en relación con la implantación de la factura electrónica.

La aplicación de estas medidas se hará sin aumento del coste de funcionamiento de los órganos afectados y no supondrá aumento del gasto público. La creación y funcionamiento

de los órganos colegiados aquí previstos será atendido con los medios personales, técnicos y presupuestarios asignados al órgano superior en el cual se encuentren integrados. Los órganos colegiados previstos ajustarán su funcionamiento a lo dispuesto en las normas contenidas en el Capítulo II del Título II de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

§ 53

Orden ESS/484/2013, de 26 de marzo, por la que se regula el Sistema de remisión electrónica de datos en el ámbito de la Seguridad Social

Ministerio de Empleo y Seguridad Social
«BOE» núm. 75, de 28 de marzo de 2013
Última modificación: 6 de marzo de 2018
Referencia: BOE-A-2013-3362

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, insta en su artículo 45.1 a las administraciones públicas a impulsar el uso y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de dichos medios establecen la Constitución y las leyes. Por su parte, el derecho de los ciudadanos a comunicarse con las administraciones por medios electrónicos se consagra con la promulgación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en la que se regula la actuación de las administraciones públicas para generalizar la sociedad de la información a través de dichos medios. En desarrollo de esta última ley, el Real Decreto 1671/2009, de 6 de noviembre, establece un marco flexible para facilitar la adaptación de organizaciones, funciones y procedimientos a la comunicación por medios electrónicos, garantizando al mismo tiempo que no resulten afectados otros bienes constitucionalmente protegidos, como son la protección de datos, los derechos de acceso a la información administrativa o la preservación de intereses de terceros.

Dentro del ámbito específico de la Administración de la Seguridad Social el uso y aplicación de técnicas y medios electrónicos para el desarrollo de su actividad y el ejercicio de sus competencias se ha regulado en la Orden de 3 de abril de 1995, sobre uso de medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, la afiliación, altas y bajas de trabajadores, la cotización y la recaudación; medios y procedimientos que, bajo la denominación «Sistema de remisión electrónica de datos (Sistema RED)», han sido objeto de implantación y desarrollo progresivo a través de sucesivas resoluciones de la Dirección General de la Tesorería General de la Seguridad Social, dictadas en aplicación de la referida Orden ministerial.

El alcance y las condiciones de utilización del Sistema RED se han ido perfilando, asimismo, al amparo de lo previsto en el artículo 30 de la Ley 50/1998, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, en aplicación del cual, por una parte, la Orden TAS/399/2004, de 12 de febrero, sobre presentación en soporte informático de los partes médicos de baja, confirmación de la baja y alta correspondientes a procesos de incapacidad temporal, ha extendido su ámbito de aplicación a la presentación de partes médicos de baja, confirmación de baja y alta correspondientes a procesos de incapacidad temporal, y, por otra parte, por la Orden TAS/1562/2005, de 25 de mayo, por la que se

establecen normas para la aplicación y desarrollo del Reglamento general de recaudación de la Seguridad Social, se determinaron los supuestos de incorporación obligatoria a dicho sistema, tras su reforma por la Orden TIN/2777/2010, de 29 de octubre, y recientemente en el ámbito del Régimen Especial del Mar se ampliaron esos supuestos por Orden ESS/229/2012, de 9 de febrero, por la que se establecen para el año 2012 las bases de cotización a la Seguridad Social de los trabajadores del Régimen Especial del Mar incluidos en los grupos segundo y tercero.

A su vez, diversas normas reglamentarias de Seguridad Social, tales como la disposición adicional quinta del Reglamento general de la gestión financiera de la Seguridad Social, aprobado por el Real Decreto 1391/1995, de 4 de agosto; la disposición adicional sexta del Reglamento general sobre cotización y liquidación de otros derechos de la Seguridad Social, aprobado por el Real Decreto 2064/1995, de 22 de diciembre; el artículo 38 del Reglamento general sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social, aprobado por el Real Decreto 84/1996, de 26 de enero y las disposiciones adicionales cuarta y quinta del Reglamento general de recaudación de la Seguridad Social, aprobado por el Real Decreto 1415/2004, de 11 de junio, también contemplan la posibilidad de utilizar los procedimientos y medios que conforman el Sistema RED para la realización de actuaciones administrativas y el suministro de datos o documentos relativos a las materias reguladas por tales reglamentos, quedando habilitada la Ministra de Empleo y Seguridad Social para determinar las condiciones de uso del citado sistema, bien de forma expresa en esos mismos preceptos o bien mediante las correspondientes disposiciones finales sobre facultades de aplicación y desarrollo de los respectivos reglamentos.

Finalmente, la disposición adicional quincuagésima del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto legislativo 1/1994, de 20 de junio, ha introducido la obligatoriedad de notificación por medios electrónicos, informáticos o telemáticos de los actos administrativos que traigan causa o se dicten como consecuencia de los datos transmitidos electrónicamente a través del Sistema RED.

En base a las referidas previsiones legales y con el objetivo de sistematizar los criterios en ellas establecidos, así como prever la extensión de la obligatoriedad de incorporación a dicho sistema al resto de las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar encuadrados en cualquiera de los regímenes del sistema de la Seguridad Social, con independencia del número de trabajadores que mantengan en alta, se considera conveniente regular en un texto único la utilización de medios electrónicos, informáticos y telemáticos en las actuaciones de inscripción de empresas, afiliación, altas, bajas y variaciones de datos de trabajadores, cotización y recaudación de empresas y trabajadores, comunicación de partes médicos de baja, de confirmación de la baja y alta correspondiente a procesos de incapacidad temporal, así como cualquier otra actuación que se determine en el ámbito de la Seguridad Social a través del Sistema RED.

Esta orden ha sido informada favorablemente por la Comisión Ministerial de Administración Electrónica del Ministerio de Empleo y Seguridad Social, al amparo de lo previsto por el artículo 2.2.e) de la Orden TIN/3155/2011, de 8 de noviembre, por la que se regula la composición y funciones del citado órgano colegiado.

En su virtud, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, y de acuerdo con el Consejo de Estado, dispongo:

Artículo 1. *Objeto y ámbito de aplicación objetivo.*

1. Esta orden tiene por objeto regular el Sistema de remisión electrónica de datos (en adelante, Sistema RED), como un servicio gestionado por la Tesorería General de la Seguridad Social para el intercambio electrónico de datos o documentos, así como para la comunicación de actuaciones administrativas entre el citado servicio común y las entidades gestoras de la Seguridad Social y los autorizados para ello, con el fin de facilitar el cumplimiento de las obligaciones de Seguridad Social por parte de los sujetos responsables en las siguientes materias:

a) Actuaciones contempladas en la normativa reguladora de la inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores, así como de la cotización y recaudación de empresas y trabajadores en el ámbito de la Seguridad Social, en los términos y condiciones previstos en cada momento por dicha normativa.

b) Comunicación de partes médicos de baja, de confirmación de la baja y de alta correspondientes a procesos de incapacidad temporal cuya gestión esté encomendada a la entidad gestora o a la mutua colaboradora con la Seguridad Social, en los términos establecidos en la Orden ESS/1187/2015, de 15 de junio, por la que se desarrolla el Real Decreto 625/2014, de 18 de julio, por el que se regulan determinados aspectos de la gestión y control de los procesos por incapacidad temporal en los primeros trescientos sesenta y cinco días de su duración.

c) Comunicación empresarial de la fecha de inicio de la suspensión del contrato de trabajo o del correspondiente permiso, a efectos de la tramitación de las prestaciones por maternidad, paternidad, riesgo durante el embarazo y riesgo durante la lactancia natural, así como de las reducciones de jornada de trabajo de los progenitores, adoptantes o acogedores, a efectos de la tramitación de la prestación de cuidado de menores afectados por cáncer u otra enfermedad grave, de las que sean beneficiarios los trabajadores por cuenta ajena o asimilados, incluidos en el respectivo régimen del sistema de la Seguridad Social.

d) Cualquier otra actuación que venga exigida en la normativa de la Seguridad Social cuya gestión esté atribuida a la Tesorería General de la Seguridad Social, en la forma y con las especificaciones técnicas que establezca por resolución de su Director General.

2. Las notificaciones de los actos administrativos que traigan causa o se dicten como consecuencia de los datos que deban comunicarse electrónicamente a través del Sistema RED se efectuarán en la sede electrónica de la Secretaría de Estado de la Seguridad Social (en adelante, SEDESS), de acuerdo con lo previsto en el artículo 132.2 del texto refundido de la Ley General de la Seguridad Social, aprobado por el Real Decreto legislativo 8/2015, de 30 de octubre, así como en la Orden ESS/485/2013, de 26 de marzo, por la que se regulan las notificaciones y comunicaciones por medios electrónicos en el ámbito de la Seguridad Social.

Artículo 2. *Ámbito de aplicación subjetivo.*

1. La incorporación al Sistema RED será obligatoria para los sujetos responsables de la obligación de cotizar a que se refiere el apartado 2 de este artículo. Los restantes sujetos responsables podrán incorporarse voluntariamente para la realización de los trámites administrativos que en cada momento permita dicho sistema para estos colectivos. En todo caso se precisará para la incorporación la autorización previa otorgada por la Tesorería General de la Seguridad Social.

2. A los efectos indicados, estarán obligados a su incorporación al Sistema RED:

a) Las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar encuadrados en el Régimen General de la Seguridad Social y en los Regímenes Especiales de la Seguridad Social de los Trabajadores del Mar y para la Minería del Carbón, con independencia del número de trabajadores que mantengan en alta y sin perjuicio de las excepciones establecidas en el apartado 3.

b) Los sujetos responsables del cumplimiento de la obligación de cotizar encuadrados en el Régimen Especial de la Seguridad Social de los Trabajadores por Cuenta Propia o Autónomos y en el Régimen Especial de la Seguridad Social de los Trabajadores del Mar como trabajadores por cuenta propia clasificados, a efectos de cotización, en el grupo primero del artículo 10 de la Ley 47/2015, de 21 de octubre, reguladora de la protección social de las personas trabajadoras del sector marítimo-pesquero, con independencia de que tengan o no trabajadores a su cargo.

En este supuesto, la incorporación al Sistema RED podrá efectuarse en los términos y condiciones de esta orden o por el uso de los medios electrónicos disponibles en la SEDESS y con arreglo a las condiciones establecidas para el acceso a sus servicios, de acuerdo con lo previsto en el artículo 3.3 de esta orden.

3. La incorporación al Sistema RED no será obligatoria:

a) En el Régimen General de la Seguridad Social, para las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar, por lo que respecta al colectivo de profesionales taurinos y al Sistema Especial para Empleados de Hogar.

b) En el Régimen Especial de la Seguridad Social de los Trabajadores del Mar, para los trabajadores por cuenta propia clasificados, a efectos de cotización, en los grupos segundo y tercero del artículo 10 de la Ley 47/2015, de 21 de octubre.

4. Las actuaciones administrativas para el intercambio de datos o documentos en el Sistema RED podrán llevarse a cabo por los sujetos responsables del cumplimiento de las obligaciones a que se refiere el artículo 1, bien en nombre propio o bien por medio de representante.

Artículo 3. *Incidencia de la incorporación efectiva al Sistema RED en la adquisición y mantenimiento de beneficios en la cotización a la Seguridad Social.*

1. Conforme a lo previsto en el párrafo primero del artículo 29 de la Ley 50/1998, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, en el caso de que las empresas, agrupaciones de empresas y demás sujetos responsables del cumplimiento de la obligación de cotizar que hubieran solicitado u obtenido reducciones, bonificaciones o cualesquiera otros beneficios en las bases, tipos y cuotas de la Seguridad Social y conceptos de recaudación conjunta, no se incorporen de manera efectiva al Sistema RED, no podrán obtener los citados beneficios y quedarán suspendidos, sin más trámite, los que tuvieran concedidos, respecto de todos sus trabajadores por cuenta ajena o asimilados y respecto de todos sus códigos de cuenta de cotización, tanto principales como secundarios, desde la fecha en que tal incorporación debió realizarse. Dicha suspensión se aplicará, asimismo, a los sujetos responsables que dejen de utilizar de forma efectiva el Sistema RED en las actuaciones relativas al encuadramiento, cotización y recaudación.

La obtención de los beneficios indicados se regirá por la normativa vigente en el período de liquidación correspondiente a la incorporación efectiva al Sistema RED y surtirá efectos desde el día primero de dicho período, sin perjuicio de la pérdida de los beneficios por el tiempo transcurrido desde el nacimiento del derecho hasta tal incorporación efectiva. Asimismo, la suspensión de aquellos beneficios quedará sin efecto y volverán a ser aplicables a partir de la liquidación correspondiente a la nueva incorporación a dicho sistema, sin que quepa la recuperación de los beneficios perdidos. Tanto en un caso como en otro, se considerará que los beneficios se han aplicado, a efectos del cómputo de su duración, durante el periodo transcurrido entre la fecha inicial en que se hubiesen podido obtener, se hubiesen obtenido o se hubiesen suspendido, y la de incorporación efectiva al Sistema RED.

No dará lugar a la pérdida de reducciones, bonificaciones o cualesquiera otros beneficios que tuvieran concedidos, la falta de transmisión de datos a través del Sistema RED por causas de carácter técnico imputables a la Tesorería General de la Seguridad Social, sin perjuicio de la obligación de presentar los documentos de cotización y los de afiliación, altas, bajas y variaciones de datos dentro de los plazos establecidos.

2. A los efectos previstos en el apartado anterior, se entiende por incorporación efectiva al Sistema RED la utilización de dicho sistema para la realización de las actuaciones previstas en el artículo 1 con plena validez y eficacia, generando los derechos y obligaciones establecidos por la normativa en vigor en relación con dichos actos, así como de cualesquiera otras exigidas en la normativa de Seguridad Social, en la forma y con los requerimientos que fije la Tesorería General de la Seguridad Social.

3. El cumplimiento de la obligación de incorporación al Sistema RED no se verá afectado cuando las actuaciones de encuadramiento, cotización y recaudación puedan realizarse a través de otros medios electrónicos distintos del citado sistema, en los términos y condiciones que fije la Tesorería General de la Seguridad Social, a fin de facilitar la prestación de los servicios electrónicos en aplicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Artículo 4. *Características del Sistema RED.*

1. El Sistema RED comprenderá las aplicaciones informáticas y telemáticas que en cada momento resulten precisas para el cumplimiento de la finalidad antes indicada, autorizándose a tal efecto la utilización de redes públicas y privadas de transmisión de datos, combinaciones de unas y otras y cualesquiera otros medios que determine la Tesorería General de la Seguridad Social.

2. El Sistema RED garantiza los siguientes principios generales:

a) Autenticación. El sistema identificará de manera inequívoca al emisor y al receptor de la información que sea distinto de la Tesorería General de la Seguridad Social, asegurando su identidad. La identificación de los interesados necesariamente se efectuará mediante sistemas de firma electrónica determinados conforme a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, así como en los artículos 13 y siguientes de la Ley 11/2007, de 22 de junio, y en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la citada ley, que resulten adecuados para garantizar su identificación, así como la autenticidad de los documentos electrónicos.

b) Constancia. El sistema dispondrá de un servicio en el que se haga constar la fecha y hora de envío de cada una de las comunicaciones realizadas entre los usuarios y la Tesorería General de la Seguridad Social.

c) Confidencialidad. El sistema garantizará que sólo el usuario acreditado debidamente tenga acceso a las comunicaciones que contengan datos de carácter personal, de acuerdo con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. A tal efecto, el sistema incluirá las pertinentes medidas de seguridad en las transmisiones mediante el cifrado de datos o a través de cualquier otro mecanismo que garantice que la información no es inteligible ni manipulable por terceros.

d) Integridad. El sistema garantizará que la información y documentos serán transmitidos sin alteración alguna de su contenido original, pudiendo ser detectada cualquier anomalía por el receptor de los mismos.

e) Conservación. El sistema garantizará la conservación de la información y documentos transmitidos durante el tiempo exigido por la normativa aplicable en función de los datos transmitidos.

f) No repudio. El sistema se instrumentará de forma que el receptor de la información o documento no pueda rechazar un envío válidamente efectuado y que el remitente tenga constancia de su recepción.

Artículo 5. *Autorización para actuar a través del Sistema RED.*

1. Para operar en el ámbito de actuación definido en el artículo 1, será necesario contar con autorización otorgada por la Tesorería General de la Seguridad Social. Dicha autorización podrá ser de dos tipos:

a) Autorización para actuar en nombre propio.

b) Autorización para actuar en nombre de otros.

La Tesorería General de la Seguridad Social determinará mediante resolución del Director General los requisitos que se han de cumplir para la obtención de cada tipo de autorización.

2. Las solicitudes de autorización serán resueltas por los directores provinciales de la Tesorería General de la Seguridad Social, informándose al autorizado de las condiciones de utilización de la autorización en el caso de resoluciones estimatorias.

El plazo máximo en que debe notificarse la resolución expresa será de tres meses, transcurrido dicho plazo podrá entenderse desestimada la solicitud por silencio administrativo.

Dicha resolución podrá ser objeto de recurso de alzada ante la Dirección General de la Tesorería General de la Seguridad Social, de acuerdo con lo establecido en los artículos 114 y 115 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya interposición suspenderá la ejecución del acto impugnado. El plazo para la interposición de dicho recurso será el de un mes a contar desde el día siguiente a la notificación. Transcurrido el plazo de tres meses

desde la interposición de dicho recurso de alzada sin que recaiga resolución expresa, el mismo podrá entenderse desestimado, según dispone el artículo 115 de la citada Ley 30/1992, de 26 de noviembre.

Las autorizaciones concedidas dejarán de surtir efectos tanto por incumplimiento de sus condiciones de utilización como por el uso abusivo o fraudulento de éstas, mediante resolución motivada de la Tesorería General de la Seguridad Social.

3. Concedida una autorización para actuar a través del Sistema RED, el autorizado quedará habilitado tanto para la transmisión electrónica de los datos o documentos a través del referido sistema como para la recepción de las comunicaciones y notificaciones de las actuaciones administrativas que se realicen al respecto, implicando esta autorización la obligación del autorizado de gestionar con carácter exclusivo mediante dicho sistema, salvo imposibilidad del servicio por causa debida a la Tesorería General de la Seguridad Social, el cumplimiento de las obligaciones y actuaciones en las materias a que se refiere el artículo 1 respecto de todos los sujetos responsables vinculados a dicha autorización, entendiéndose realizadas directamente por estos últimos.

4. Las actuaciones a las que habilita la autorización RED para la transmisión electrónica de datos o documentos y recepción de las comunicaciones y notificaciones de las actuaciones administrativas consecuencia de dicha transmisión, podrán ser realizadas tanto por el autorizado como por los usuarios que éste designe a través del correspondiente servicio establecido al efecto por la Tesorería General de la Seguridad Social, garantizándose conforme al artículo 4.2.a) la identificación del emisor o receptor y la autenticidad e integridad de los datos y documentos objeto de transmisión.

En todo caso, las transmisiones de datos o documentos realizadas por los usuarios a través del Sistema RED, así como las comunicaciones y las notificaciones de las actuaciones administrativas que éstos reciban de la Tesorería General de la Seguridad Social, se entenderán transmitidos y recibidos por el autorizado.

Artículo 6. *Requisitos para el ejercicio efectivo de las autorizaciones RED.*

Para el intercambio efectivo de los datos o documentos y recepción de las comunicaciones y notificaciones de las actuaciones administrativas que traigan causa o se dicten como consecuencia de los datos que deban comunicarse a través del Sistema RED, correspondientes a sujetos responsables, se requiere:

a) En el caso de autorizaciones para actuar en nombre propio, la comunicación por el medio que establezca al efecto la Tesorería General de la Seguridad Social de los códigos de cuenta de cotización o números de afiliación cuyos datos hayan de ser transmitidos a través del Sistema RED.

b) En el caso de autorizaciones para actuar en nombre de terceros, además de la comunicación a que se refiere el párrafo anterior, será necesaria la acreditación de la representación otorgada por los sujetos responsables en cuyo nombre se actúe, a favor del autorizado y de sus usuarios, por el medio que establezca la Tesorería General de la Seguridad Social.

Artículo 7. *Responsabilidad de los autorizados.*

La responsabilidad de las actuaciones realizadas recae en todo caso sobre el autorizado, con independencia de quien las efectúe, y sin perjuicio de la responsabilidad que éste pueda exigir a los usuarios responsables de la actuación.

Se prohíbe expresamente al autorizado RED y a los usuarios designados por éste el tratamiento automatizado de los datos a los que tengan acceso mediante la creación de ficheros informáticos para fines distintos de los estrictamente propios del Sistema RED.

Será responsabilidad del autorizado mantener actualizada la relación de usuarios acreditados a operar en el sistema, en el marco de su autorización.

Artículo 8. *Efectos de la transmisión electrónica de datos o documentos a través del Sistema RED.*

1. La remisión electrónica de datos o documentos relativos a actuaciones de inscripción de empresas, afiliación, altas, bajas y variaciones de datos de trabajadores, cotización y

recaudación de empresas y trabajadores en el ámbito de la Seguridad Social y la comunicación de partes médicos de baja, de confirmación de la baja y de alta correspondientes a procesos de incapacidad temporal a través del Sistema RED, así como la transmisión de las actuaciones administrativas realizadas por la Tesorería General de la Seguridad Social o entidad gestora correspondiente, que se deriven de la citada transmisión, gozarán de plena validez y eficacia, generando los derechos y obligaciones establecidos por la normativa en vigor en relación con dichos actos.

2. La obligación de informar sobre los datos figurados en las relaciones nominales de trabajadores (documentos serie TC-2) que se transmitan por el Sistema RED, prevista en el artículo 25.4 del Reglamento general de recaudación de la Seguridad Social, aprobado por el Real Decreto 1415/2004, de 11 de junio, se considerará cumplida de acuerdo con lo dispuesto en dicho artículo, mediante la colocación o puesta a disposición de los trabajadores, a través de la presentación en pantalla de ordenador o terminal informático, de los datos de sus archivos que, a tales efectos, serán considerados como copia autorizada de las citadas relaciones nominales de trabajadores, siempre que, en este último caso, se muestren acompañados de su correspondiente huella electrónica.

3. En el supuesto de falta de ingreso de las obligaciones de pago correspondientes, la aportación en soporte informático de los datos de las relaciones nominales de trabajadores efectuada en plazo reglamentario se considerará como presentación de documentos de cotización a los efectos previstos en el artículo 26 del texto refundido de la Ley General de la Seguridad Social.

4. La utilización del Sistema RED para el suministro de datos se entenderá sin perjuicio del cumplimiento, por parte de las empresas y demás sujetos responsables, de las demás obligaciones previstas en el Reglamento general sobre inscripción de empresas y afiliación, altas, bajas y variaciones de datos de trabajadores en la Seguridad Social, aprobado por el Real Decreto 84/1996, de 26 de enero.

Artículo 9. *Validez de los documentos generados por impresión autorizada de las actuaciones tramitadas electrónicamente a través del Sistema RED.*

Los documentos generados por impresión autorizada de las actuaciones tramitadas electrónicamente a través del Sistema RED incluirán elementos de contraste/cotejo y gozarán de la misma validez y eficacia frente a terceros que las certificaciones expedidas al respecto por los órganos competentes de la Tesorería General de la Seguridad Social.

La Tesorería General de la Seguridad Social podrá realizar la impresión de los datos y documentos recibidos, producidos y emitidos por el Sistema RED, considerándose como impresión de contraste y gozando de la misma validez que los originales tramitados.

La autenticidad e integridad de los documentos generados podrá verificarse mediante los sistemas dispuestos a tal efecto, consistentes en la verificación mediante el código electrónico de autenticidad (CEA), mediante huella digital o cualquier otro sistema que permita contrastar la información de dichos documentos con la obrante en las correspondientes bases de datos corporativas.

Artículo 10. *Conexión y modalidades de trabajo.*

1. La conexión para el intercambio electrónico de datos o documentos se realizará a través de internet.

Excepcionalmente, la Tesorería General de la Seguridad Social podrá autorizar a determinados sujetos responsables con un elevado número de trabajadores, a optar por una modalidad de intercambio electrónico de datos bajo protocolo «ad hoc». Asimismo, por la Tesorería General de la Seguridad Social podrá determinarse igualmente, en función de otros criterios objetivos, qué autorizados utilizarán un determinado protocolo para el intercambio de datos.

2. Las modalidades de trabajo utilizadas por el Sistema RED son dos:

a) Conexión directa con la Tesorería General de la Seguridad Social.

b) Envío y recepción de ficheros con una estructura determinada, según instrucciones técnicas que figuran en la página web de la Seguridad Social.

La Tesorería General de la Seguridad Social podrá incluir cualquier otro protocolo o modalidad de trabajo que la evolución tecnológica aconseje, así como la supresión de los utilizados hasta el momento.

Disposición adicional primera. *Exención de la obligación de presentación de la relación nominal de trabajadores.*

En aquellos supuestos en los que existiendo transmisión electrónica de la relación nominal de trabajadores a través del Sistema RED, y por razones técnicas la Tesorería General de la Seguridad Social no pueda calcular la liquidación correspondiente, no será necesario adjuntar, para su sellado y validación, dicha relación nominal de trabajadores (documentos serie TC-2) al boletín de cotización (serie TC-1) en el momento del ingreso de las cuotas en cualquiera de las oficinas recaudadoras autorizadas. Al respecto, en la casilla del boletín de cotización (serie TC-1) reservada a firma y sello del empresario se indicará:

«No acompaña TC-2

Autorización TGSS número..... de fecha.....»

Disposición adicional segunda. *Servicio de asistencia y orientación para la cumplimentación de las actuaciones de encuadramiento, cotización y recaudación por medios electrónicos.*

En el marco de lo previsto por el artículo 8 de la Ley 11/2007, de 22 de junio, la Tesorería General de la Seguridad Social pondrá a disposición de las empresas, agrupaciones de empresas y demás sujetos responsables obligados a incorporarse de manera efectiva al Sistema RED, que por sus dificultades personales o su reducida dimensión y localización geográfica así lo requieran, un servicio de asistencia técnica y asesoramiento, que incluirá los medios necesarios para garantizar la efectividad del cumplimiento de la obligación de transmisión electrónica de los datos de encuadramiento, cotización y recaudación impuesta por el artículo 1.1.

Dicho servicio se prestará siempre que el sujeto responsable no disponga de la correspondiente autorización para transmitir por el Sistema RED, en los términos y condiciones que determine la Tesorería General de la Seguridad Social.

Disposición transitoria única. *Autorizaciones para actuar a través del Sistema RED otorgadas con anterioridad a la fecha de entrada en vigor de esta orden.*

Respecto a las autorizaciones para actuar a través del Sistema RED otorgadas con anterioridad a la fecha de entrada en vigor de esta orden a profesionales colegiados y terceros que viniesen transmitiendo electrónicamente a través del Sistema RED datos relativos a una o varias empresas, agrupaciones de empresas y demás sujetos responsables, serán válidas, salvo manifestación expresa en contrario, y sin perjuicio de que la Tesorería General de la Seguridad Social pueda en cualquier momento solicitar la acreditación de la representación, procediendo a dejar sin efecto la autorización respecto de las empresas o sujetos obligados en el caso de que no se acredite suficientemente ésta.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogadas todas las disposiciones de igual o inferior rango en tanto contradigan o se opongan a lo establecido en esta orden.

2. Quedan derogadas expresamente las siguientes disposiciones:

a) La Orden de 3 de abril de 1995, sobre uso de medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, afiliación, altas y bajas de trabajadores, cotización y recaudación en el ámbito de la Seguridad Social.

b) De la Orden TAS/1562/2005, de 25 de mayo, por la que se establecen normas para la aplicación y desarrollo del Reglamento general de recaudación de la Seguridad Social, aprobado por el Real Decreto 1415/2004, de 11 de junio, el artículo 28 y las disposiciones adicionales cuarta y quinta.

c) De la Orden ESS/229/2012, de 9 de febrero, por la que se establecen para el año 2012 las bases de cotización a la Seguridad Social de los trabajadores del Régimen Especial del Mar incluidos en los grupos segundo y tercero, los apartados 1 y 2 de su disposición adicional única.

Disposición final primera. *Título competencial.*

Esta orden se dicta al amparo de lo dispuesto en el artículo 149.1.17.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de legislación básica y régimen económico de la Seguridad Social.

Disposición final segunda. *Facultades de aplicación y desarrollo.*

Se faculta al Director General de la Tesorería General de la Seguridad Social para dictar cuantas resoluciones resulten necesarias para la aplicación de lo dispuesto en esta orden.

Disposición final tercera. *Entrada en vigor.*

La presente orden entrará en vigor el día 1 del mes siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 54

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

Jefatura del Estado
«BOE» núm. 295, de 10 de diciembre de 2013
Última modificación: 9 de julio de 2022
Referencia: BOE-A-2013-12887

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley:

PREÁMBULO

I

La transparencia, el acceso a la información pública y las normas de buen gobierno deben ser los ejes fundamentales de toda acción política. Sólo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos.

Los países con mayores niveles en materia de transparencia y normas de buen gobierno cuentan con instituciones más fuertes, que favorecen el crecimiento económico y el desarrollo social. En estos países, los ciudadanos pueden juzgar mejor y con más criterio la capacidad de sus responsables públicos y decidir en consecuencia. Permitiendo una mejor fiscalización de la actividad pública se contribuye a la necesaria regeneración democrática, se promueve la eficiencia y eficacia del Estado y se favorece el crecimiento económico.

La presente Ley tiene un triple alcance: incrementa y refuerza la transparencia en la actividad pública –que se articula a través de obligaciones de publicidad activa para todas las Administraciones y entidades públicas–, reconoce y garantiza el acceso a la información –regulado como un derecho de amplio ámbito subjetivo y objetivo– y establece las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias jurídicas derivadas de su incumplimiento –lo que se convierte en una exigencia de responsabilidad para todos los que desarrollan actividades de relevancia pública–.

En estas tres vertientes, la Ley supone un importante avance en la materia y establece unos estándares homologables al del resto de democracias consolidadas. En definitiva, constituye un paso fundamental y necesario que se verá acompañado en el futuro con el impulso y adhesión por parte del Estado tanto a iniciativas multilaterales en este ámbito como con la firma de los instrumentos internacionales ya existentes en esta materia.

II

En el ordenamiento jurídico español ya existen normas sectoriales que contienen obligaciones concretas de publicidad activa para determinados sujetos. Así, por ejemplo, en materia de contratos, subvenciones, presupuestos o actividades de altos cargos nuestro país cuenta con un destacado nivel de transparencia. Sin embargo, esta regulación resulta insuficiente en la actualidad y no satisface las exigencias sociales y políticas del momento. Por ello, con esta Ley se avanza y se profundiza en la configuración de obligaciones de publicidad activa que, se entiende, han de vincular a un amplio número de sujetos entre los que se encuentran todas las Administraciones Públicas, los órganos del Poder Legislativo y Judicial en lo que se refiere a sus actividades sujetas a Derecho Administrativo, así como otros órganos constitucionales y estatutarios. Asimismo, la Ley se aplicará a determinadas entidades que, por su especial relevancia pública, o por su condición de perceptores de fondos públicos, vendrán obligados a reforzar la transparencia de su actividad.

La Ley amplía y refuerza las obligaciones de publicidad activa en distintos ámbitos. En materia de información institucional, organizativa y de planificación exige a los sujetos comprendidos en su ámbito de aplicación la publicación de información relativa a las funciones que desarrollan, la normativa que les resulta de aplicación y su estructura organizativa, además de sus instrumentos de planificación y la evaluación de su grado de cumplimiento. En materia de información de relevancia jurídica y que afecte directamente al ámbito de las relaciones entre la Administración y los ciudadanos, la ley contiene un amplio repertorio de documentos que, al ser publicados, proporcionarán una mayor seguridad jurídica. Igualmente, en el ámbito de la información de relevancia económica, presupuestaria y estadística, se establece un amplio catálogo que debe ser accesible y entendible para los ciudadanos, dado su carácter de instrumento óptimo para el control de la gestión y utilización de los recursos públicos. Por último, se establece la obligación de publicar toda la información que con mayor frecuencia sea objeto de una solicitud de acceso, de modo que las obligaciones de transparencia se cohonesten con los intereses de la ciudadanía.

Para canalizar la publicación de tan ingente cantidad de información y facilitar el cumplimiento de estas obligaciones de publicidad activa y, desde la perspectiva de que no se puede, por un lado, hablar de transparencia y, por otro, no poner los medios adecuados para facilitar el acceso a la información divulgada, la Ley contempla la creación y desarrollo de un Portal de la Transparencia. Las nuevas tecnologías nos permiten hoy día desarrollar herramientas de extraordinaria utilidad para el cumplimiento de las disposiciones de la Ley cuyo uso permita que, a través de un único punto de acceso, el ciudadano pueda obtener toda la información disponible.

La Ley también regula el derecho de acceso a la información pública que, no obstante, ya ha sido desarrollado en otras disposiciones de nuestro ordenamiento. En efecto, partiendo de la previsión contenida en el artículo 105.b) de nuestro texto constitucional, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, desarrolla en su artículo 37 el derecho de los ciudadanos a acceder a los registros y documentos que se encuentren en los archivos administrativos. Pero esta regulación adolece de una serie de deficiencias que han sido puestas de manifiesto de forma reiterada al no ser claro el objeto del derecho de acceso, al estar limitado a documentos contenidos en procedimientos administrativos ya terminados y al resultar su ejercicio extraordinariamente limitado en su articulación práctica.

Igualmente, pero con un alcance sectorial y derivado de sendas Directivas comunitarias, otras normas contemplan el acceso a la información pública. Es el caso de la Ley 27/2006, de 18 de julio, por la que se regulan los derechos de acceso a la información, de participación pública y de acceso a la justicia en materia de medio ambiente y de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, que regula el uso privado de documentos en poder de Administraciones y organismos del

sector público. Además, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, a la vez que reconoce el derecho de los ciudadanos a relacionarse con la Administración por medios electrónicos, se sitúa en un camino en el que se avanza con esta Ley: la implantación de una cultura de transparencia que impone la modernización de la Administración, la reducción de cargas burocráticas y el empleo de los medios electrónicos para la facilitar la participación, la transparencia y el acceso a la información.

La Ley, por lo tanto, no parte de la nada ni colma un vacío absoluto, sino que ahonda en lo ya conseguido, supliendo sus carencias, subsanando sus deficiencias y creando un marco jurídico acorde con los tiempos y los intereses ciudadanos.

Desde la perspectiva del Derecho comparado, tanto la Unión Europea como la mayoría de sus Estados miembros cuentan ya en sus ordenamientos jurídicos con una legislación específica que regula la transparencia y el derecho de acceso a la información pública. España no podía permanecer por más tiempo al margen y, tomando como ejemplo los modelos que nos proporcionan los países de nuestro entorno, adopta esta nueva regulación.

En lo que respecta a buen gobierno, la Ley supone un avance de extraordinaria importancia. Principios meramente programáticos y sin fuerza jurídica se incorporan a una norma con rango de ley y pasan a informar la interpretación y aplicación de un régimen sancionador al que se encuentran sujetos todos los responsables públicos entendidos en sentido amplio que, con independencia del Gobierno del que formen parte o de la Administración en la que presten sus servicios y, precisamente por las funciones que realizan, deben ser un modelo de ejemplaridad en su conducta.

III

El título I de la Ley regula e incrementa la transparencia de la actividad de todos los sujetos que prestan servicios públicos o ejercen potestades administrativas mediante un conjunto de previsiones que se recogen en dos capítulos diferenciados y desde una doble perspectiva: la publicidad activa y el derecho de acceso a la información pública.

El ámbito subjetivo de aplicación de este título, recogido en su capítulo I, es muy amplio e incluye a todas las Administraciones Públicas, organismos autónomos, agencias estatales, entidades públicas empresariales y entidades de derecho público, en la medida en que tengan atribuidas funciones de regulación o control sobre un determinado sector o actividad, así como a las entidades de Derecho Público con personalidad jurídica propia, vinculadas o dependientes de cualquiera de las Administraciones Públicas, incluidas las Universidades públicas. En relación con sus actividades sujetas a Derecho Administrativo, la Ley se aplica también a las Corporaciones de Derecho Público, a la Casa de Su Majestad el Rey, al Congreso de los Diputados, al Senado, al Tribunal Constitucional y al Consejo General del Poder Judicial, así como al Banco de España, Consejo de Estado, al Defensor del Pueblo, al Tribunal de Cuentas, al Consejo Económico y Social y las instituciones autonómicas análogas. También se aplica a las sociedades mercantiles en cuyo capital social la participación directa o indirecta de las entidades mencionadas sea superior al cincuenta por ciento, a las fundaciones del sector público y a las asociaciones constituidas por las Administraciones, organismos y entidades a las que se ha hecho referencia. Asimismo, se aplicará a los partidos políticos, organizaciones sindicales y organizaciones empresariales y a todas las entidades privadas que perciban una determinada cantidad de ayudas o subvenciones públicas. Por último, las personas que presten servicios públicos o ejerzan potestades administrativas también están obligadas a suministrar a la Administración a la que se encuentren vinculadas, previo requerimiento, toda la información necesaria para el cumplimiento por aquélla de las obligaciones de esta Ley. Esta obligación es igualmente aplicable a los adjudicatarios de contratos del sector público.

El capítulo II, dedicado a la publicidad activa, establece una serie de obligaciones para los sujetos incluidos en el ámbito de aplicación del título I, que habrán de difundir determinada información sin esperar una solicitud concreta de los administrados. En este punto se incluyen datos sobre información institucional, organizativa y de planificación, de relevancia jurídica y de naturaleza económica, presupuestaria y estadística.

Para favorecer de forma decidida el acceso de todos a la información que se difunda se creará el Portal de la Transparencia, que incluirá, además de la información sobre la que

existe una obligación de publicidad activa, aquella cuyo acceso se solicite con mayor frecuencia. El Portal será un punto de encuentro y de difusión, que muestra una nueva forma de entender el derecho de los ciudadanos a acceder a la información pública. Se prevé además en este punto que la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las entidades que integran la Administración Local puedan adoptar medidas de colaboración para el cumplimiento de sus obligaciones de publicidad activa.

El capítulo III configura de forma amplia el derecho de acceso a la información pública, del que son titulares todas las personas y que podrá ejercerse sin necesidad de motivar la solicitud. Este derecho solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información –derivado de lo dispuesto en la Constitución Española– o por su entrada en conflicto con otros intereses protegidos. En todo caso, los límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad. Asimismo, dado que el acceso a la información puede afectar de forma directa a la protección de los datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios. Así, por un lado, en la medida en que la información afecte directamente a la organización o actividad pública del órgano prevalecerá el acceso, mientras que, por otro, se protegen –como no puede ser de otra manera– los datos que la normativa califica como especialmente protegidos, para cuyo acceso se requerirá, con carácter general, el consentimiento de su titular.

Con objeto de facilitar el ejercicio del derecho de acceso a la información pública la Ley establece un procedimiento ágil, con un breve plazo de respuesta, y dispone la creación de unidades de información en la Administración General del Estado, lo que facilita el conocimiento por parte del ciudadano del órgano ante el que deba presentarse la solicitud así como del competente para la tramitación.

En materia de impugnaciones se crea una reclamación potestativa y previa a la vía judicial de la que conocerá el Consejo de Transparencia y Buen Gobierno, organismo de naturaleza independiente de nueva creación, y que sustituye a los recursos administrativos.

El título II otorga rango de Ley a los principios éticos y de actuación que deben regir la labor de los miembros del Gobierno y altos cargos y asimilados de la Administración del Estado, de las Comunidades Autónomas y de las Entidades Locales. Igualmente, se clarifica y refuerza el régimen sancionador que les resulta de aplicación, en consonancia con la responsabilidad a la que están sujetos.

Este sistema busca que los ciudadanos cuenten con servidores públicos que ajusten sus actuaciones a los principios de eficacia, austeridad, imparcialidad y, sobre todo, de responsabilidad. Para cumplir este objetivo, la Ley consagra un régimen sancionador estructurado en tres ámbitos: infracciones en materia de conflicto de intereses, en materia de gestión económico-presupuestaria y en el ámbito disciplinario. Además, se incorporan infracciones derivadas del incumplimiento de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera. En el ámbito económico-presupuestario resulta destacable que se impondrán sanciones a quienes comprometan gastos, liquiden obligaciones y ordenen pagos sin crédito suficiente para realizarlos o con infracción de lo dispuesto en la normativa presupuestaria, o no justifiquen la inversión de los fondos a los que se refieren la normativa presupuestaria equivalente. De esta manera se introduce un mecanismo de control fundamental que evitará comportamientos irresponsables y que resultan inaceptables en un Estado de Derecho.

La comisión de las infracciones previstas dará lugar a la imposición de sanciones como la destitución en los cargos públicos que ocupe el infractor, la no percepción de pensiones indemnizatorias, la obligación de restituir las cantidades indebidamente percibidas y la obligación de indemnizar a la Hacienda Pública. Debe señalarse que estas sanciones se inspiran en las ya previstas en la Ley 5/2006, de 10 de abril, de conflictos de intereses de miembros del Gobierno y de los altos cargos de la Administración General del Estado.

Además, se establece la previsión de que los autores de infracciones muy graves no puedan ser nombrados para ocupar determinados cargos públicos durante un periodo de entre 5 y 10 años.

El título III de la Ley crea y regula el Consejo de Transparencia y Buen Gobierno, un órgano independiente al que se le otorgan competencias de promoción de la cultura de transparencia en la actividad de la Administración Pública, de control del cumplimiento de las obligaciones de publicidad activa, así como de garantía del derecho de acceso a la información pública y de la observancia de las disposiciones de buen gobierno. Se crea, por lo tanto, un órgano de supervisión y control para garantizar la correcta aplicación de la Ley.

El Consejo de Transparencia y Buen Gobierno se configura como un órgano independiente, con plena capacidad jurídica y de obrar y cuenta con una estructura sencilla que, a la vez que garantiza su especialización y operatividad, evita crear grandes estructuras administrativas. La independencia y autonomía en el ejercicio de sus funciones vendrá garantizada, asimismo, por el respaldo parlamentario con el que deberá contar el nombramiento de su Presidente.

Para respetar al máximo las competencias autonómicas, expresamente se prevé que el Consejo de Transparencia y Buen Gobierno sólo tendrá competencias en aquellas Comunidades Autónomas con las que haya firmado Convenio al efecto, quedando, en otro caso, en manos del órgano autonómico que haya sido designado las competencias que a nivel estatal asume el Consejo.

Las disposiciones adicionales abordan diversas cuestiones como la aplicación de regulaciones especiales del derecho de acceso, la revisión y simplificación normativa –en el entendido de que también es un ejercicio de buen gobierno y una manifestación más de la transparencia el clarificar la normativa que está vigente y es de aplicación– y la colaboración entre el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos en la determinación de criterios para la aplicación de los preceptos de la ley en lo relativo a la protección de datos personales.

Las disposiciones finales, entre otras cuestiones, modifican la regulación del derecho de acceso a los archivos y registros administrativos contenida en la Ley 30/1992, de 26 de noviembre, amplían la publicidad de determinada información que figura en el Registro de bienes y derechos patrimoniales de los altos cargos de la Administración General del Estado y la obligación de publicidad prevista en el apartado 4 del artículo 136 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Por último, la Ley prevé una entrada en vigor escalonada atendiendo a las especiales circunstancias que conllevará la aplicación de sus diversas disposiciones.

TÍTULO PRELIMINAR

Artículo 1. *Objeto.*

Esta Ley tiene por objeto ampliar y reforzar la transparencia de la actividad pública, regular y garantizar el derecho de acceso a la información relativa a aquella actividad y establecer las obligaciones de buen gobierno que deben cumplir los responsables públicos así como las consecuencias derivadas de su incumplimiento.

TÍTULO I

Transparencia de la actividad pública

CAPÍTULO I

Ámbito subjetivo de aplicación

Artículo 2. *Ámbito subjetivo de aplicación.*

1. Las disposiciones de este título se aplicarán a:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla y las entidades que integran la Administración Local.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.

c) Los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad.

d) Las entidades de Derecho Público con personalidad jurídica propia, vinculadas a cualquiera de las Administraciones Públicas o dependientes de ellas, incluidas las Universidades públicas.

e) Las corporaciones de Derecho Público, en lo relativo a sus actividades sujetas a Derecho Administrativo.

f) La Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo.

g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100.

h) Las fundaciones del sector público previstas en la legislación en materia de fundaciones.

i) Las asociaciones constituidas por las Administraciones, organismos y entidades previstos en este artículo. Se incluyen los órganos de cooperación previstos en el artículo 5 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en la medida en que, por su peculiar naturaleza y por carecer de una estructura administrativa propia, le resulten aplicables las disposiciones de este título. En estos casos, el cumplimiento de las obligaciones derivadas de la presente Ley serán llevadas a cabo por la Administración que ostente la Secretaría del órgano de cooperación.

2. A los efectos de lo previsto en este título, se entiende por Administraciones Públicas los organismos y entidades incluidos en las letras a) a d) del apartado anterior.

Artículo 3. *Otros sujetos obligados.*

Las disposiciones del capítulo II de este título serán también aplicables a:

a) Los partidos políticos, organizaciones sindicales y organizaciones empresariales.

b) Las entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40 % del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros.

Artículo 4. *Obligación de suministrar información.*

Las personas físicas y jurídicas distintas de las referidas en los artículos anteriores que presten servicios públicos o ejerzan potestades administrativas estarán obligadas a suministrar a la Administración, organismo o entidad de las previstas en el artículo 2.1 a la que se encuentren vinculadas, previo requerimiento, toda la información necesaria para el cumplimiento por aquéllos de las obligaciones previstas en este título. Esta obligación se extenderá a los adjudicatarios de contratos del sector público en los términos previstos en el respectivo contrato.

CAPÍTULO II

Publicidad activa

Artículo 5. *Principios generales.*

1. Los sujetos enumerados en el artículo 2.1 publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública.

2. Las obligaciones de transparencia contenidas en este capítulo se entienden sin perjuicio de la aplicación de la normativa autonómica correspondiente o de otras disposiciones específicas que prevean un régimen más amplio en materia de publicidad.

3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos.

4. La información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados y, preferiblemente, en formatos reutilizables. Se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada así como su identificación y localización.

Cuando se trate de entidades sin ánimo de lucro que persigan exclusivamente fines de interés social o cultural y cuyo presupuesto sea inferior a 50.000 euros, el cumplimiento de las obligaciones derivadas de esta Ley podrá realizarse utilizando los medios electrónicos puestos a su disposición por la Administración Pública de la que provenga la mayor parte de las ayudas o subvenciones públicas percibidas.

5. Toda la información será comprensible, de acceso fácil y gratuito y estará a disposición de las personas con discapacidad en una modalidad suministrada por medios o en formatos adecuados de manera que resulten accesibles y comprensibles, conforme al principio de accesibilidad universal y diseño para todos.

Artículo 6. *Información institucional, organizativa y de planificación.*

1. Los sujetos comprendidos en el ámbito de aplicación de este título publicarán información relativa a las funciones que desarrollan, la normativa que les sea de aplicación así como a su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a los responsables de los diferentes órganos y su perfil y trayectoria profesional.

2. Las Administraciones Públicas publicarán los planes y programas anuales y plurianuales en los que se fijen objetivos concretos, así como las actividades, medios y tiempo previsto para su consecución. Su grado de cumplimiento y resultados deberán ser objeto de evaluación y publicación periódica junto con los indicadores de medida y valoración, en la forma en que se determine por cada Administración competente.

En el ámbito de la Administración General del Estado corresponde a las inspecciones generales de servicios la evaluación del cumplimiento de estos planes y programas.

Artículo 6 bis. *Registro de actividades de tratamiento.*

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.

Artículo 7. *Información de relevancia jurídica.*

Las Administraciones Públicas, en el ámbito de sus competencias, publicarán:

a) Las directrices, instrucciones, acuerdos, circulares o respuestas a consultas planteadas por los particulares u otros órganos en la medida en que supongan una interpretación del Derecho o tengan efectos jurídicos.

b) Los Anteproyectos de Ley y los proyectos de Decretos Legislativos cuya iniciativa les corresponda, cuando se soliciten los dictámenes a los órganos consultivos correspondientes. En el caso en que no sea preceptivo ningún dictamen la publicación se realizará en el momento de su aprobación.

c) Los proyectos de Reglamentos cuya iniciativa les corresponda. Cuando sea preceptiva la solicitud de dictámenes, la publicación se producirá una vez que estos hayan sido solicitados a los órganos consultivos correspondientes sin que ello suponga, necesariamente, la apertura de un trámite de audiencia pública.

d) Las memorias e informes que conformen los expedientes de elaboración de los textos normativos, en particular, la memoria del análisis de impacto normativo regulada por el Real Decreto 1083/2009, de 3 de julio.

e) Los documentos que, conforme a la legislación sectorial vigente, deban ser sometidos a un período de información pública durante su tramitación.

Artículo 8. *Información económica, presupuestaria y estadística.*

1. Teniendo en cuenta las competencias legislativas de las Comunidades Autónomas, los sujetos incluidos en el ámbito de aplicación de este título deberán hacer pública, como mínimo, la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria que se indican a continuación:

a) Todos los contratos, con indicación del objeto, duración, el importe de la licitación y de adjudicación, el procedimiento utilizado para su celebración, los instrumentos a través de los que, en su caso, se ha publicitado, el número de licitadores participantes en el procedimiento y la identidad del adjudicatario, así como las modificaciones del contrato. Igualmente serán objeto de publicación las decisiones de desistimiento y renuncia de los contratos. La publicación de la información relativa a los contratos menores podrá realizarse trimestralmente.

Asimismo, se publicarán datos estadísticos sobre el porcentaje en volumen presupuestario de contratos adjudicados a través de cada uno de los procedimientos previstos en la legislación de contratos del sector público.

Además, se publicará información estadística sobre el porcentaje de participación en contratos adjudicados, tanto en relación con su número como en relación con su valor, de la categoría de microempresas, pequeñas y medianas empresas (pymes), entendidas como tal según el anexo I del Reglamento (UE) n.º 651/2014 de la Comisión, de 17 de junio de 2014, para cada uno de los procedimientos y tipologías previstas en la legislación de contratos del sector público. La publicación de esta información se realizará semestralmente, a partir de un año de la publicación de la norma.

b) La relación de los convenios suscritos, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, obligados a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas. Igualmente, se publicarán las encomiendas de gestión que se firmen, con indicación de su objeto, presupuesto, duración, obligaciones económicas y las subcontrataciones que se realicen con mención de los adjudicatarios, procedimiento seguido para la adjudicación e importe de la misma.

c) Las subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios.

d) Los presupuestos, con descripción de las principales partidas presupuestarias e información actualizada y comprensible sobre su estado de ejecución y sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las Administraciones Públicas.

e) Las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo que sobre ellos se emitan.

f) Las retribuciones percibidas anualmente por los altos cargos y máximos responsables de las entidades incluidas en el ámbito de la aplicación de este título. Igualmente, se harán públicas las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo.

g) Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos así como las que autoricen el ejercicio de actividad privada al cese de

los altos cargos de la Administración General del Estado o asimilados según la normativa autonómica o local.

h) Las declaraciones anuales de bienes y actividades de los representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares.

i) La información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia, en los términos que defina cada administración competente.

2. Los sujetos mencionados en el artículo 3 deberán publicar la información a la que se refieren las letras a) y b) del apartado primero de este artículo cuando se trate de contratos o convenios celebrados con una Administración Pública. Asimismo, habrán de publicar la información prevista en la letra c) en relación a las subvenciones que reciban cuando el órgano concedente sea una Administración Pública.

3. Las Administraciones Públicas publicarán la relación de los bienes inmuebles que sean de su propiedad o sobre los que ostenten algún derecho real.

Artículo 9. *Control.*

1. El cumplimiento por la Administración General del Estado de las obligaciones contenidas en este capítulo será objeto de control por parte del Consejo de Transparencia y Buen Gobierno.

2. En ejercicio de la competencia prevista en el apartado anterior, el Consejo de Transparencia y Buen Gobierno, de acuerdo con el procedimiento que se prevea reglamentariamente, podrá dictar resoluciones en las que se establezcan las medidas que sea necesario adoptar para el cese del incumplimiento y el inicio de las actuaciones disciplinarias que procedan.

3. El incumplimiento reiterado de las obligaciones de publicidad activa reguladas en este capítulo tendrá la consideración de infracción grave a los efectos de aplicación a sus responsables del régimen disciplinario previsto en la correspondiente normativa reguladora.

Artículo 10. *Portal de la Transparencia.*

1. La Administración General del Estado desarrollará un Portal de la Transparencia, dependiente del Ministerio de la Presidencia, que facilitará el acceso de los ciudadanos a toda la información a la que se refieren los artículos anteriores relativa a su ámbito de actuación.

2. El Portal de la Transparencia incluirá, en los términos que se establezcan reglamentariamente, la información de la Administración General del Estado, cuyo acceso se solicite con mayor frecuencia.

3. La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla y las entidades que integran la Administración Local podrán adoptar otras medidas complementarias y de colaboración para el cumplimiento de las obligaciones de transparencia recogidas en este capítulo.

Artículo 11. *Principios técnicos.*

El Portal de la Transparencia contendrá información publicada de acuerdo con las prescripciones técnicas que se establezcan reglamentariamente que deberán adecuarse a los siguientes principios:

a) Accesibilidad: se proporcionará información estructurada sobre los documentos y recursos de información con vistas a facilitar la identificación y búsqueda de la información.

b) Interoperabilidad: la información publicada será conforme al Esquema Nacional de Interoperabilidad, aprobado por el Real Decreto 4/2010, de 8 enero, así como a las normas técnicas de interoperabilidad.

c) Reutilización: se fomentará que la información sea publicada en formatos que permita su reutilización, de acuerdo con lo previsto en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público y en su normativa de desarrollo.

CAPÍTULO III

Derecho de acceso a la información pública

Sección 1.ª Régimen general

Artículo 12. *Derecho de acceso a la información pública.*

Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley.

Asimismo, y en el ámbito de sus respectivas competencias, será de aplicación la correspondiente normativa autonómica.

Artículo 13. *Información pública.*

Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones.

Artículo 14. *Límites al derecho de acceso.*

1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para:

a) La seguridad nacional.
b) La defensa.
c) Las relaciones exteriores.
d) La seguridad pública.
e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios.
f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva.
g) Las funciones administrativas de vigilancia, inspección y control.
h) Los intereses económicos y comerciales.
i) La política económica y monetaria.
j) El secreto profesional y la propiedad intelectual e industrial.
k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión.
l) La protección del medio ambiente.

2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso.

3. Las resoluciones que de conformidad con lo previsto en la sección 2.ª se dicten en aplicación de este artículo serán objeto de publicidad previa disociación de los datos de carácter personal que contuvieran y sin perjuicio de lo dispuesto en el apartado 3 del artículo 20, una vez hayan sido notificadas a los interesados.

Artículo 15. *Protección de datos personales.*

1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos

a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.

2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano.

3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal.

Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios:

a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español.

b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos.

d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad.

4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas.

5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso.

Artículo 16. *Acceso parcial.*

En los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida.

Sección 2.ª Ejercicio del derecho de acceso a la información pública

Artículo 17. *Solicitud de acceso a la información.*

1. El procedimiento para el ejercicio del derecho de acceso se iniciará con la presentación de la correspondiente solicitud, que deberá dirigirse al titular del órgano administrativo o entidad que posea la información. Cuando se trate de información en posesión de personas físicas o jurídicas que presten servicios públicos o ejerzan potestades administrativas, la solicitud se dirigirá a la Administración, organismo o entidad de las previstas en el artículo 2.1 a las que se encuentren vinculadas.

2. La solicitud podrá presentarse por cualquier medio que permita tener constancia de:

a) La identidad del solicitante.
b) La información que se solicita.
c) Una dirección de contacto, preferentemente electrónica, a efectos de comunicaciones.
d) En su caso, la modalidad que se prefiera para acceder a la información solicitada.

3. El solicitante no está obligado a motivar su solicitud de acceso a la información. Sin embargo, podrá exponer los motivos por los que solicita la información y que podrán ser

tenidos en cuenta cuando se dicte la resolución. No obstante, la ausencia de motivación no será por si sola causa de rechazo de la solicitud.

4. Los solicitantes de información podrán dirigirse a las Administraciones Públicas en cualquiera de las lenguas cooficiales del Estado en el territorio en el que radique la Administración en cuestión.

Artículo 18. *Causas de inadmisión.*

1. Se inadmitirán a trámite, mediante resolución motivada, las solicitudes:

a) Que se refieran a información que esté en curso de elaboración o de publicación general.

b) Referidas a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas.

c) Relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración.

d) Dirigidas a un órgano en cuyo poder no obre la información cuando se desconozca el competente.

e) Que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta Ley.

2. En el caso en que se inadmita la solicitud por concurrir la causa prevista en la letra d) del apartado anterior, el órgano que acuerde la inadmisión deberá indicar en la resolución el órgano que, a su juicio, es competente para conocer de la solicitud.

Artículo 19. *Tramitación.*

1. Si la solicitud se refiere a información que no obre en poder del sujeto al que se dirige, éste la remitirá al competente, si lo conociera, e informará de esta circunstancia al solicitante.

2. Cuando la solicitud no identifique de forma suficiente la información, se pedirá al solicitante que la concrete en un plazo de diez días, con indicación de que, en caso de no hacerlo, se le tendrá por desistido, así como de la suspensión del plazo para dictar resolución.

3. Si la información solicitada pudiera afectar a derechos o intereses de terceros, debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas. El solicitante deberá ser informado de esta circunstancia, así como de la suspensión del plazo para dictar resolución hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación.

4. Cuando la información objeto de la solicitud, aun obrando en poder del sujeto al que se dirige, haya sido elaborada o generada en su integridad o parte principal por otro, se le remitirá la solicitud a éste para que decida sobre el acceso.

Artículo 20. *Resolución.*

1. La resolución en la que se conceda o deniegue el acceso deberá notificarse al solicitante y a los terceros afectados que así lo hayan solicitado en el plazo máximo de un mes desde la recepción de la solicitud por el órgano competente para resolver.

Este plazo podrá ampliarse por otro mes en el caso de que el volumen o la complejidad de la información que se solicita así lo hagan necesario y previa notificación al solicitante.

2. Serán motivadas las resoluciones que denieguen el acceso, las que concedan el acceso parcial o a través de una modalidad distinta a la solicitada y las que permitan el acceso cuando haya habido oposición de un tercero. En este último supuesto, se indicará expresamente al interesado que el acceso sólo tendrá lugar cuando haya transcurrido el plazo del artículo 22.2.

3. Cuando la mera indicación de la existencia o no de la información supusiera la vulneración de alguno de los límites al acceso se indicará esta circunstancia al desestimarse la solicitud.

4. Transcurrido el plazo máximo para resolver sin que se haya dictado y notificado resolución expresa se entenderá que la solicitud ha sido desestimada.

5. Las resoluciones dictadas en materia de acceso a la información pública son recurribles directamente ante la Jurisdicción Contencioso-administrativa, sin perjuicio de la posibilidad de interposición de la reclamación potestativa prevista en el artículo 24.

6. El incumplimiento reiterado de la obligación de resolver en plazo tendrá la consideración de infracción grave a los efectos de la aplicación a sus responsables del régimen disciplinario previsto en la correspondiente normativa reguladora.

Artículo 21. *Unidades de información.*

1. Las Administraciones Públicas incluidas en el ámbito de aplicación de este título establecerán sistemas para integrar la gestión de solicitudes de información de los ciudadanos en el funcionamiento de su organización interna.

2. En el ámbito de la Administración General del Estado, existirán unidades especializadas que tendrán las siguientes funciones:

a) Recabar y difundir la información a la que se refiere el capítulo II del título I de esta Ley.

b) Recibir y dar tramitación a las solicitudes de acceso a la información.

c) Realizar los trámites internos necesarios para dar acceso a la información solicitada.

d) Realizar el seguimiento y control de la correcta tramitación de las solicitudes de acceso a la información.

e) Llevar un registro de las solicitudes de acceso a la información.

f) Asegurar la disponibilidad en la respectiva página web o sede electrónica de la información cuyo acceso se solicita con más frecuencia.

g) Mantener actualizado un mapa de contenidos en el que queden identificados los distintos tipos de información que obre en poder del órgano.

h) Todas aquellas que sean necesarias para asegurar una correcta aplicación de las disposiciones de esta Ley.

3. El resto de las entidades incluidas en el ámbito de aplicación de este título identificarán claramente el órgano competente para conocer de las solicitudes de acceso.

Artículo 22. *Formalización del acceso.*

1. El acceso a la información se realizará preferentemente por vía electrónica, salvo cuando no sea posible o el solicitante haya señalado expresamente otro medio. Cuando no pueda darse el acceso en el momento de la notificación de la resolución deberá otorgarse, en cualquier caso, en un plazo no superior a diez días.

2. Si ha existido oposición de tercero, el acceso sólo tendrá lugar cuando, habiéndose concedido dicho acceso, haya transcurrido el plazo para interponer recurso contencioso administrativo sin que se haya formalizado o haya sido resuelto confirmando el derecho a recibir la información.

3. Si la información ya ha sido publicada, la resolución podrá limitarse a indicar al solicitante cómo puede acceder a ella.

4. El acceso a la información será gratuito. No obstante, la expedición de copias o la trasposición de la información a un formato diferente al original podrá dar lugar a la exigencia de exacciones en los términos previstos en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, o, en su caso, conforme a la normativa autonómica o local que resulte aplicable.

Sección 3.ª Régimen de impugnaciones

Artículo 23. *Recursos.*

1. La reclamación prevista en el artículo siguiente tendrá la consideración de sustitutiva de los recursos administrativos de conformidad con lo dispuesto en el artículo 107.2 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2. No obstante lo dispuesto en el apartado anterior, contra las resoluciones dictadas por los órganos previstos en el artículo 2.1.f) sólo cabrá la interposición de recurso contencioso-administrativo.

Artículo 24. *Reclamación ante el Consejo de Transparencia y Buen Gobierno.*

1. Frente a toda resolución expresa o presunta en materia de acceso podrá interponerse una reclamación ante el Consejo de Transparencia y Buen Gobierno, con carácter potestativo y previo a su impugnación en vía contencioso-administrativa.

2. La reclamación se interpondrá en el plazo de un mes a contar desde el día siguiente al de la notificación del acto impugnado o desde el día siguiente a aquel en que se produzcan los efectos del silencio administrativo.

3. La tramitación de la reclamación se ajustará a lo dispuesto en materia de recursos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Cuando la denegación del acceso a la información se fundamente en la protección de derechos o intereses de terceros se otorgará, previamente a la resolución de la reclamación, trámite de audiencia a las personas que pudieran resultar afectadas para que aleguen lo que a su derecho convenga.

4. El plazo máximo para resolver y notificar la resolución será de tres meses, transcurrido el cual, la reclamación se entenderá desestimada.

5. Las resoluciones del Consejo de Transparencia y Buen Gobierno se publicarán, previa disociación de los datos de carácter personal que contuvieran, por medios electrónicos y en los términos en que se establezca reglamentariamente, una vez se hayan notificado a los interesados.

El Presidente del Consejo de Transparencia y Buen Gobierno comunicará al Defensor del Pueblo las resoluciones que dicte en aplicación de este artículo.

6. La competencia para conocer de dichas reclamaciones corresponderá al Consejo de Transparencia y Buen Gobierno, salvo en aquellos supuestos en que las Comunidades Autónomas atribuyan dicha competencia a un órgano específico, de acuerdo con lo establecido en la disposición adicional cuarta de esta Ley.

TÍTULO II

Buen gobierno

Artículo 25. *Ámbito de aplicación.*

1. En el ámbito de la Administración General del Estado las disposiciones de este título se aplicarán a los miembros del Gobierno, a los Secretarios de Estado y al resto de los altos cargos de la Administración General del Estado y de las entidades del sector público estatal, de Derecho público o privado, vinculadas o dependientes de aquella.

A estos efectos, se considerarán altos cargos los que tengan tal consideración en aplicación de la normativa en materia de conflictos de intereses.

2. Este título será de aplicación a los altos cargos o asimilados que, de acuerdo con la normativa autonómica o local que sea de aplicación, tengan tal consideración, incluidos los miembros de las Juntas de Gobierno de las Entidades Locales.

3. La aplicación a los sujetos mencionados en los apartados anteriores de las disposiciones contenidas en este título no afectará, en ningún caso, a la condición de cargo electo que pudieran ostentar.

Artículo 26. *Principios de buen gobierno.*

1. Las personas comprendidas en el ámbito de aplicación de este título observarán en el ejercicio de sus funciones lo dispuesto en la Constitución Española y en el resto del ordenamiento jurídico y promoverán el respeto a los derechos fundamentales y a las libertades públicas.

2. Asimismo, adecuarán su actividad a los siguientes:

a) Principios generales:

1.º Actuarán con transparencia en la gestión de los asuntos públicos, de acuerdo con los principios de eficacia, economía y eficiencia y con el objetivo de satisfacer el interés general.

2.º Ejercerán sus funciones con dedicación al servicio público, absteniéndose de cualquier conducta que sea contraria a estos principios.

3.º Respetarán el principio de imparcialidad, de modo que mantengan un criterio independiente y ajeno a todo interés particular.

4.º Asegurarán un trato igual y sin discriminaciones de ningún tipo en el ejercicio de sus funciones.

5.º Actuarán con la diligencia debida en el cumplimiento de sus obligaciones y fomentarán la calidad en la prestación de servicios públicos.

6.º Mantendrán una conducta digna y tratarán a los ciudadanos con esmerada corrección.

7.º Asumirán la responsabilidad de las decisiones y actuaciones propias y de los organismos que dirigen, sin perjuicio de otras que fueran exigibles legalmente.

b) Principios de actuación:

1.º Desempeñarán su actividad con plena dedicación y con pleno respeto a la normativa reguladora de las incompatibilidades y los conflictos de intereses.

2.º Guardarán la debida reserva respecto a los hechos o informaciones conocidos con motivo u ocasión del ejercicio de sus competencias.

3.º Pondrán en conocimiento de los órganos competentes cualquier actuación irregular de la cual tengan conocimiento.

4.º Ejercerán los poderes que les atribuye la normativa vigente con la finalidad exclusiva para la que fueron otorgados y evitarán toda acción que pueda poner en riesgo el interés público o el patrimonio de las Administraciones.

5.º No se implicarán en situaciones, actividades o intereses incompatibles con sus funciones y se abstendrán de intervenir en los asuntos en que concurra alguna causa que pueda afectar a su objetividad.

6.º No aceptarán para sí regalos que superen los usos habituales, sociales o de cortesía, ni favores o servicios en condiciones ventajosas que puedan condicionar el desarrollo de sus funciones. En el caso de obsequios de una mayor relevancia institucional se procederá a su incorporación al patrimonio de la Administración Pública correspondiente.

7.º Desempeñarán sus funciones con transparencia.

8.º Gestionarán, protegerán y conservarán adecuadamente los recursos públicos, que no podrán ser utilizados para actividades que no sean las permitidas por la normativa que sea de aplicación.

9.º No se valdrán de su posición en la Administración para obtener ventajas personales o materiales.

3. Los principios establecidos en este artículo informarán la interpretación y aplicación del régimen sancionador regulado en este título.

Artículo 27. *Infracciones y sanciones en materia de conflicto de intereses.*

El incumplimiento de las normas de incompatibilidades o de las que regulan las declaraciones que han de realizar las personas comprendidas en el ámbito de este título será sancionado de conformidad con lo dispuesto en la normativa en materia de conflictos de intereses de la Administración General del Estado y para el resto de Administraciones de acuerdo con su propia normativa que resulte de aplicación.

Artículo 28. *Infracciones en materia de gestión económico-presupuestaria.*

Constituyen infracciones muy graves las siguientes conductas cuando sean culpables:

a) La incursión en alcance en la administración de los fondos públicos cuando la conducta no sea subsumible en ninguno de los tipos que se contemplan en las letras siguientes.

b) La administración de los recursos y demás derechos de la Hacienda Pública sin sujeción a las disposiciones que regulan su liquidación, recaudación o ingreso en el Tesoro.

c) Los compromisos de gastos, reconocimiento de obligaciones y ordenación de pagos sin crédito suficiente para realizarlos o con infracción de lo dispuesto en la Ley 47/2003, de 26 de noviembre, General Presupuestaria, o en la de Presupuestos u otra normativa presupuestaria que sea aplicable.

d) La omisión del trámite de intervención previa de los gastos, obligaciones o pagos, cuando ésta resulte preceptiva o del procedimiento de resolución de discrepancias frente a los reparos suspensivos de la intervención, regulado en la normativa presupuestaria.

e) La ausencia de justificación de la inversión de los fondos a los que se refieren los artículos 78 y 79 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, o, en su caso, la normativa presupuestaria equivalente de las administraciones distintas de la General del Estado.

f) El incumplimiento de la obligación de destinar íntegramente los ingresos obtenidos por encima de los previstos en el presupuesto a la reducción del nivel de deuda pública de conformidad con lo previsto en el artículo 12.5 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera y el incumplimiento de la obligación del destino del superávit presupuestario a la reducción del nivel de endeudamiento neto en los términos previstos en el artículo 32 y la disposición adicional sexta de la citada Ley.

g) La realización de operaciones de crédito y emisiones de deudas que no cuenten con la preceptiva autorización o, habiéndola obtenido, no se cumpla con lo en ella previsto o se superen los límites previstos en la Ley Orgánica 2/2012, de 27 de abril, la Ley Orgánica 8/1980, de 22 de septiembre, de Financiación de las Comunidades Autónomas, y en el Texto Refundido de la Ley Reguladora de las Haciendas Locales, aprobado por el Real Decreto Legislativo 2/2004, de 5 de marzo.

h) La no adopción en plazo de las medidas necesarias para evitar el riesgo de incumplimiento, cuando se haya formulado la advertencia prevista en el artículo 19 de la Ley Orgánica 2/2012, de 27 de abril.

i) La suscripción de un Convenio de colaboración o concesión de una subvención a una Administración Pública que no cuente con el informe favorable del Ministerio de Hacienda y Administraciones Públicas previsto en el artículo 20.3 de la Ley Orgánica 2/2012, de 27 de abril.

j) La no presentación o la falta de puesta en marcha en plazo del plan económico-financiero o del plan de reequilibrio de conformidad con el artículo 23 de la Ley Orgánica 2/2012, de 27 de abril.

k) El incumplimiento de las obligaciones de publicación o de suministro de información previstas en la normativa presupuestaria y económico-financiera, siempre que en este último caso se hubiera formulado requerimiento.

l) La falta de justificación de la desviación, o cuando así se le haya requerido la falta de inclusión de nuevas medidas en el plan económico-financiero o en el plan de reequilibrio de acuerdo con el artículo 24.3 de la Ley Orgánica 2/2012, de 27 de abril.

m) La no adopción de las medidas previstas en los planes económico-financieros y de reequilibrio, según corresponda, previstos en los artículos 21 y 22 de la Ley Orgánica 2/2012, de 27 de abril.

n) La no adopción en el plazo previsto del acuerdo de no disponibilidad al que se refieren los artículos 20.5.a) y 25 de la Ley Orgánica 2/2012, de 27 de abril, así como la no constitución del depósito previsto en el citado artículo 25 de la misma Ley, cuando así se haya solicitado.

ñ) La no adopción de un acuerdo de no disponibilidad, la no constitución del depósito que se hubiere solicitado o la falta de ejecución de las medidas propuestas por la Comisión de Expertos cuando se hubiere formulado el requerimiento del Gobierno previsto en el artículo 26.1 de la Ley Orgánica 2/2012, de 27 de abril.

o) El incumplimiento de las instrucciones dadas por el Gobierno para ejecutar las medidas previstas en el artículo 26.1 de la Ley Orgánica 2/2012, de 27 de abril.

p) El incumplimiento de la obligación de rendir cuentas regulada en el artículo 137 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria u otra normativa presupuestaria que sea aplicable.

Artículo 29. *Infracciones disciplinarias.*

1. Son infracciones muy graves:

a) El incumplimiento del deber de respeto a la Constitución y a los respectivos Estatutos de Autonomía de las Comunidades Autónomas y Ciudades de Ceuta y Melilla, en el ejercicio de sus funciones.

b) Toda actuación que suponga discriminación por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual, lengua, opinión, lugar de nacimiento o vecindad, sexo o cualquier otra condición o circunstancia personal o social, así como el acoso por razón de origen racial o étnico, religión o convicciones, discapacidad, edad u orientación sexual y el acoso moral, sexual y por razón de sexo.

c) La adopción de acuerdos manifiestamente ilegales que causen perjuicio grave a la Administración o a los ciudadanos.

d) La publicación o utilización indebida de la documentación o información a que tengan o hayan tenido acceso por razón de su cargo o función.

e) La negligencia en la custodia de secretos oficiales, declarados así por Ley o clasificados como tales, que sea causa de su publicación o que provoque su difusión o conocimiento indebido.

f) El notorio incumplimiento de las funciones esenciales inherentes al puesto de trabajo o funciones encomendadas.

g) La violación de la imparcialidad, utilizando las facultades atribuidas para influir en procesos electorales de cualquier naturaleza y ámbito.

h) La prevalencia de la condición de alto cargo para obtener un beneficio indebido para sí o para otro.

i) La obstaculización al ejercicio de las libertades públicas y derechos sindicales.

j) La realización de actos encaminados a coartar el libre ejercicio del derecho de huelga.

k) El acoso laboral.

l) La comisión de una infracción grave cuando el autor hubiera sido sancionado por dos infracciones graves a lo largo del año anterior contra las que no quepa recurso en la vía administrativa.

2. Son infracciones graves:

a) El abuso de autoridad en el ejercicio del cargo.

b) La intervención en un procedimiento administrativo cuando se dé alguna de las causas de abstención legalmente señaladas.

c) La emisión de informes y la adopción de acuerdos manifiestamente ilegales cuando causen perjuicio a la Administración o a los ciudadanos y no constituyan infracción muy grave.

d) No guardar el debido sigilo respecto a los asuntos que se conozcan por razón del cargo, cuando causen perjuicio a la Administración o se utilice en provecho propio.

e) El incumplimiento de los plazos u otras disposiciones de procedimiento en materia de incompatibilidades, cuando no suponga el mantenimiento de una situación de incompatibilidad.

f) La comisión de una infracción leve cuando el autor hubiera sido sancionado por dos infracciones leves a lo largo del año anterior contra las que no quepa recurso en la vía administrativa.

3. Son infracciones leves:

a) La incorrección con los superiores, compañeros o subordinados.

b) El descuido o negligencia en el ejercicio de sus funciones y el incumplimiento de los principios de actuación del artículo 26.2.b) cuando ello no constituya infracción grave o muy grave o la conducta no se encuentre tipificada en otra norma.

Artículo 30. *Sanciones.*

1. Las infracciones leves serán sancionadas con una amonestación.

2. Por la comisión de una infracción grave se impondrán al infractor algunas de las siguientes sanciones:

a) La declaración del incumplimiento y su publicación en el «Boletín Oficial del Estado» o diario oficial que corresponda.

b) La no percepción, en el caso de que la llevara aparejada, de la correspondiente indemnización para el caso de cese en el cargo.

3. En el caso de las infracciones muy graves, se impondrán en todo caso las sanciones previstas en el apartado anterior.

4. Los sancionados por la comisión de una infracción muy grave serán destituidos del cargo que ocupen salvo que ya hubiesen cesado y no podrán ser nombrados para ocupar ningún puesto de alto cargo o asimilado durante un periodo de entre cinco y diez años con arreglo a los criterios previstos en el apartado siguiente.

5. La comisión de infracciones muy graves, graves o leves se sancionará de acuerdo con los criterios recogidos en el artículo 131.3 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y los siguientes:

a) La naturaleza y entidad de la infracción.

b) La gravedad del peligro ocasionado o del perjuicio causado.

c) Las ganancias obtenidas, en su caso, como consecuencia de los actos u omisiones constitutivos de la infracción.

d) Las consecuencias desfavorables de los hechos para la Hacienda Pública respectiva.

e) La circunstancia de haber procedido a la subsanación de la infracción por propia iniciativa.

f) La reparación de los daños o perjuicios causados.

En la graduación de las sanciones se valorará la existencia de perjuicios para el interés público, la repercusión de la conducta en los ciudadanos, y, en su caso, la percepción indebida de cantidades por el desempeño de actividades públicas incompatibles.

6. Cuando las infracciones pudieran ser constitutivas de delito, la Administración pondrá los hechos en conocimiento del Fiscal General del Estado y se abstendrá de seguir el procedimiento mientras la autoridad judicial no dicte una resolución que ponga fin al proceso penal.

7. Cuando los hechos estén tipificados como infracción en una norma administrativa especial, se dará cuenta de los mismos a la Administración competente para la instrucción del correspondiente procedimiento sancionador, suspendiéndose las actuaciones hasta la terminación de aquel. No se considerará normativa especial la Ley 47/2003, de 26 de noviembre, General Presupuestaria, respecto de las infracciones previstas en el artículo 28, pudiéndose tramitar el procedimiento de responsabilidad patrimonial simultáneamente al procedimiento sancionador.

8. En todo caso la comisión de las infracciones previstas en el artículo 28 conllevará las siguientes consecuencias:

a) La obligación de restituir, en su caso, las cantidades percibidas o satisfechas indebidamente.

b) La obligación de indemnizar a la Hacienda Pública en los términos del artículo 176 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 31. *Órgano competente y procedimiento.*

1. El procedimiento sancionador se iniciará de oficio, por acuerdo del órgano competente, bien por propia iniciativa o como consecuencia de orden superior, petición razonada de otros órganos o denuncia de los ciudadanos.

La responsabilidad será exigida en procedimiento administrativo instruido al efecto, sin perjuicio de dar conocimiento de los hechos al Tribunal de Cuentas por si procediese, en su caso, la incoación del oportuno procedimiento de responsabilidad contable.

2. El órgano competente para ordenar la incoación será:

a) Cuando el alto cargo tenga la condición de miembro del Gobierno o de Secretario de Estado, el Consejo de Ministros a propuesta del Ministro de Hacienda y Administraciones Públicas.

b) Cuando los presuntos responsables sean personas al servicio de la Administración General del Estado distintas de los anteriores, el Ministro de Hacienda y Administraciones Públicas.

c) Cuando los presuntos responsables sean personas al servicio de la Administración autonómica o local, la orden de incoación del procedimiento se dará por los órganos que tengan atribuidas estas funciones en aplicación del régimen disciplinario propio de las Comunidades Autónomas o Entidades Locales en las que presten servicios los cargos contra los que se dirige el procedimiento.

3. En los supuestos previstos en las letras a) y b) del apartado anterior, la instrucción de los correspondientes procedimientos corresponderá a la Oficina de Conflictos de Intereses. En el supuesto contemplado en el apartado c) la instrucción corresponderá al órgano competente en aplicación del régimen disciplinario propio de la Comunidad Autónoma o Entidad Local correspondiente.

4. La competencia para la imposición de sanciones corresponderá:

a) Al Consejo de Ministros cuando el alto cargo tenga la condición de miembro del Gobierno o Secretario de Estado.

b) Al Ministro de Hacienda y Administraciones Públicas cuando el responsable sea un alto cargo de la Administración General del Estado.

c) Cuando el procedimiento se dirija contra altos cargos de las Comunidades Autónomas o Entidades Locales, los órganos que tengan atribuidas estas funciones en aplicación del régimen disciplinario propio de Administraciones en las que presten servicios los cargos contra los que se dirige el procedimiento o, en su caso, el Consejo de Gobierno de la Comunidad Autónoma o el Pleno de la Junta de Gobierno de la Entidad Local de que se trate.

5. Las resoluciones que se dicten en aplicación del procedimiento sancionador regulado en este título serán recurribles ante el orden jurisdiccional contencioso-administrativo.

Artículo 32. *Prescripción.*

1. El plazo de prescripción de las infracciones previstas en este título será de cinco años para las infracciones muy graves, tres años para las graves y un año para las leves.

2. Las sanciones impuestas por la comisión de infracciones muy graves prescribirán a los cinco años, las impuestas por infracciones graves a los tres años y las que sean consecuencia de la comisión de infracciones leves prescribirán en el plazo de un año.

3. Para el cómputo de los plazos de prescripción regulados en los dos apartados anteriores, así como para las causas de su interrupción, se estará a lo dispuesto en el artículo 132 de la Ley 30/1992, de 30 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

TÍTULO III

Consejo de Transparencia y Buen Gobierno

Artículo 33. *Consejo de Transparencia y Buen Gobierno.*

1. Se crea el Consejo de Transparencia y Buen Gobierno como organismo público de los previstos en la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado. Estará adscrito al Ministerio de Hacienda y Administraciones Públicas.

2. El Consejo de Transparencia y Buen Gobierno tiene personalidad jurídica propia y plena capacidad de obrar. Actúa con autonomía y plena independencia en el cumplimiento de sus fines.

Artículo 34. *Fines.*

El Consejo de Transparencia y Buen Gobierno tiene por finalidad promover la transparencia de la actividad pública, velar por el cumplimiento de las obligaciones de

publicidad, salvaguardar el ejercicio de derecho de acceso a la información pública y garantizar la observancia de las disposiciones de buen gobierno.

Artículo 35. *Composición.*

El Consejo de Transparencia y Buen Gobierno estará compuesto por los siguientes órganos:

a) La Comisión de Transparencia y Buen Gobierno.
b) El Presidente del Consejo de Transparencia y Buen Gobierno que lo será también de su Comisión.

Artículo 36. *Comisión de Transparencia y Buen Gobierno.*

1. La Comisión de Transparencia y Buen Gobierno ejercerá todas las competencias que le asigna esta Ley, así como aquellas que les sean atribuidas en su normativa de desarrollo.
2. Dicha Comisión estará compuesta por:

a) El Presidente.
b) Un Diputado.
c) Un Senador.
d) Un representante del Tribunal de Cuentas.
e) Un representante del Defensor del Pueblo.
f) Un representante de la Agencia Española de Protección de Datos.
g) Un representante de la Secretaría de Estado de Administraciones Públicas.
h) Un representante de la Autoridad Independiente de Responsabilidad Fiscal.

3. La condición de miembro de la Comisión del Consejo de Transparencia y Buen Gobierno no exigirá dedicación exclusiva ni dará derecho a remuneración con excepción de lo previsto en el artículo siguiente.
4. Al menos una vez al año, la Comisión de Transparencia y Buen Gobierno convocará a los representantes de los organismos que, con funciones similares a las desarrolladas por ella, hayan sido creados por las Comunidades Autónomas en ejercicio de sus competencias. A esta reunión podrá ser convocado un representante de la Administración Local propuesto por la Federación Española de Municipios y Provincias.

Artículo 37. *Presidente del Consejo de Transparencia y Buen Gobierno.*

1. El Presidente del Consejo de Transparencia y Buen Gobierno será nombrado por un período no renovable de cinco años mediante Real Decreto, a propuesta del titular del Ministerio de Hacienda y Administraciones Públicas, entre personas de reconocido prestigio y competencia profesional previa comparecencia de la persona propuesta para el cargo ante la Comisión correspondiente del Congreso de los Diputados. El Congreso, a través de la Comisión competente y por acuerdo adoptado por mayoría absoluta, deberá refrendar el nombramiento del candidato propuesto en el plazo de un mes natural desde la recepción de la correspondiente comunicación.
2. El Presidente del Consejo de Transparencia y Buen Gobierno cesará en su cargo por la expiración de su mandato, a petición propia o por separación acordada por el Gobierno, previa instrucción del correspondiente procedimiento por el titular del Ministerio de Hacienda y Administraciones Públicas, por incumplimiento grave de sus obligaciones, incapacidad permanente para el ejercicio de su función, incompatibilidad sobrevenida o condena por delito doloso.
3. El Presidente del Consejo de Transparencia y Buen Gobierno percibirá las retribuciones fijadas de acuerdo con el Real Decreto 451/2012, de 5 de marzo, por el que se regula el régimen retributivo de los máximos responsables y directivos en el sector público empresarial y otras entidades.

Artículo 38. *Funciones.*

1. Para la consecución de sus objetivos, el Consejo de Transparencia y Buen Gobierno tiene encomendadas las siguientes funciones:

a) Adoptar recomendaciones para el mejor cumplimiento de las obligaciones contenidas en esta Ley.

b) Asesorar en materia de transparencia, acceso a la información pública y buen gobierno.

c) Informar preceptivamente los proyectos normativos de carácter estatal que desarrollen esta Ley o que estén relacionados con su objeto.

d) Evaluar el grado de aplicación de esta Ley. Para ello, elaborará anualmente una memoria en la que se incluirá información sobre el cumplimiento de las obligaciones previstas y que será presentada ante las Cortes Generales.

e) Promover la elaboración de borradores de recomendaciones y de directrices y normas de desarrollo de buenas prácticas en materia de transparencia, acceso a la información pública y buen gobierno.

f) Promover actividades de formación y sensibilización para un mejor conocimiento de las materias reguladas por esta Ley.

g) Colaborar, en las materias que le son propias, con órganos de naturaleza análoga.

h) Aquellas otras que le sean atribuidas por norma de rango legal o reglamentario.

2. El Presidente del Consejo de Transparencia y Buen Gobierno ejercerá las siguientes funciones:

a) Adoptar criterios de interpretación uniforme de las obligaciones contenidas en esta Ley.

b) Velar por el cumplimiento de las obligaciones de publicidad contenidas en el capítulo II del título I de acuerdo con lo previsto en el artículo 9 de esta Ley.

c) Conocer de las reclamaciones que se presenten en aplicación del artículo 24 de esta Ley.

d) Responder las consultas que, con carácter facultativo, le planteen los órganos encargados de tramitar y resolver las solicitudes de acceso a la información.

e) Instar el inicio del procedimiento sancionador previsto en el título II de esta Ley. El órgano competente deberá motivar, en su caso, su decisión de no incoar el procedimiento.

f) Aprobar el anteproyecto de presupuesto.

g) Aquellas otras que le sean atribuidas por norma de rango legal o reglamentario.

Artículo 39. *Régimen jurídico.*

1. El Consejo de Transparencia y Buen Gobierno se regirá, además de por lo dispuesto en esta Ley, por:

a) Las disposiciones de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, que le sean de aplicación. Anualmente elaborará un anteproyecto de presupuesto con la estructura que establezca el Ministerio de Hacienda y Administraciones Públicas para su elevación al Gobierno y su posterior integración en los Presupuestos Generales del Estado.

b) El Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público.

c) La Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas, y, en lo no previsto en ella, por el Derecho privado en sus adquisiciones patrimoniales.

d) La Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, y las demás normas aplicables al personal funcionario de la Administración General del Estado, en materia de medios personales.

e) La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y por la normativa que le sea de aplicación, en lo no dispuesto por esta Ley, cuando desarrolle sus funciones públicas.

2. El Consejo de Ministros aprobará mediante Real Decreto el Estatuto del Consejo de Transparencia y Buen Gobierno, en el que se establecerá su organización, estructura, funcionamiento, así como todos los aspectos que sean necesarios para el cumplimiento de sus funciones.

3. Con carácter general, los puestos de trabajo del Consejo de Transparencia y Buen Gobierno serán desempeñados por funcionarios públicos de acuerdo con lo establecido en la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público, y las normas de

función pública aplicables al personal funcionario de la Administración General del Estado. El personal laboral podrá desempeñar puestos de trabajo que se ajusten a la normativa de función pública de la Administración General del Estado. Asimismo, el personal que pase a prestar servicios en el Consejo de Transparencia y Buen Gobierno mediante los procedimientos de provisión previstos en la Administración General del Estado mantendrá la condición de personal funcionario o laboral, de acuerdo con la legislación aplicable.

4. El Consejo de Transparencia y Buen Gobierno contará para el cumplimiento de sus fines con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargos a los Presupuestos Generales del Estado.

b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

c) Cualesquiera otros que legalmente puedan serle atribuidos.

Artículo 40. *Relaciones con las Cortes Generales.*

El Consejo de Transparencia y Buen Gobierno elevará anualmente a las Cortes Generales una memoria sobre el desarrollo de sus actividades y sobre el grado de cumplimiento de las disposiciones establecidas en esta Ley. El Presidente del Consejo de Transparencia y Buen Gobierno comparecerá ante la Comisión correspondiente para dar cuenta de tal memoria, así como cuantas veces sea requerido para ello.

Disposición adicional primera. *Regulaciones especiales del derecho de acceso a la información pública.*

1. La normativa reguladora del correspondiente procedimiento administrativo será la aplicable al acceso por parte de quienes tengan la condición de interesados en un procedimiento administrativo en curso a los documentos que se integren en el mismo.

2. Se regirán por su normativa específica, y por esta Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.

3. En este sentido, esta Ley será de aplicación, en lo no previsto en sus respectivas normas reguladoras, al acceso a la información ambiental y a la destinada a la reutilización.

Disposición adicional segunda. *Revisión y simplificación normativa.*

1. La Administración General del Estado acometerá una revisión, simplificación y, en su caso, una consolidación normativa de su ordenamiento jurídico. Para ello, habrá de efectuar los correspondientes estudios, derogar las normas que hayan quedado obsoletas y determinar, en su caso, la necesidad de introducir modificaciones, novedades o proponer la elaboración de un texto refundido, de conformidad con las previsiones constitucionales y legales sobre competencia y procedimiento a seguir, según el rango de las normas que queden afectadas.

2. A tal fin, la Secretaría de Estado de Relaciones con las Cortes elaborará un Plan de Calidad y Simplificación Normativa y se encargará de coordinar el proceso de revisión y simplificación normativa respecto del resto de Departamentos ministeriales.

3. Las Secretarías Generales Técnicas de los diferentes Departamentos ministeriales llevarán a cabo el proceso de revisión y simplificación en sus ámbitos competenciales de actuación, pudiendo coordinar su actividad con los órganos competentes de las Comunidades Autónomas que, en ejercicio de las competencias que le son propias y en aplicación del principio de cooperación administrativa, lleven a cabo un proceso de revisión de sus respectivos ordenamientos jurídicos.

Disposición adicional tercera. *Corporaciones de Derecho Público.*

Para el cumplimiento de las obligaciones previstas en el título I de esta Ley, las corporaciones de Derecho Público podrán celebrar convenios de colaboración con la Administración Pública correspondiente o, en su caso, con el organismo que ejerza la representación en su ámbito concreto de actividad.

Disposición adicional cuarta. *Reclamación.*

1. La resolución de la reclamación prevista en el artículo 24 corresponderá, en los supuestos de resoluciones dictadas por las Administraciones de las Comunidades Autónomas y su sector público, y por las Entidades Locales comprendidas en su ámbito territorial, al órgano independiente que determinen las Comunidades Autónomas.

No obstante lo dispuesto en el párrafo anterior, contra las resoluciones dictadas por las Asambleas Legislativas y las instituciones análogas al Consejo de Estado, Consejo Económico y Social, Tribunal de Cuentas y Defensor del Pueblo en el caso de esas mismas reclamaciones sólo cabrá la interposición de recurso contencioso-administrativo.

2. Las Comunidades Autónomas podrán atribuir la competencia para la resolución de la reclamación prevista en el artículo 24 al Consejo de Transparencia y Buen Gobierno. A tal efecto, deberán celebrar el correspondiente convenio con la Administración General del Estado, en el que se estipulen las condiciones en que la Comunidad sufragará los gastos derivados de esta asunción de competencias.

3. Las Ciudades con Estatuto de Autonomía podrán designar sus propios órganos independientes o bien atribuir la competencia al Consejo de Transparencia y Buen Gobierno, celebrando al efecto un Convenio en los términos previstos en el apartado anterior.

Disposición adicional quinta. *Colaboración con la Agencia Española de Protección de Datos.*

El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre.

Disposición adicional sexta. *Información de la Casa de Su Majestad el Rey.*

La Secretaría General de la Presidencia del Gobierno será el órgano competente para tramitar el procedimiento mediante en el que se solicite el acceso a la información que obre en poder de la Casa de Su Majestad el Rey, así como para conocer de cualquier otra cuestión que pudiera surgir derivada de la aplicación por este órgano de las disposiciones de esta Ley.

Disposición adicional séptima.

El Gobierno aprobará un plan formativo en el ámbito de la transparencia dirigido a los funcionarios y personal de la Administración General del Estado, acompañado, a su vez, de una campaña informativa dirigida a los ciudadanos. El Gobierno incorporará al sector público estatal en el Plan Nacional de Responsabilidad Social Corporativa.

Disposición adicional octava.

El Congreso de los Diputados, el Senado y las Asambleas Legislativas de las Comunidades Autónomas regularán en sus respectivos reglamentos la aplicación concreta de las disposiciones de esta Ley.

Disposición final primera. *Modificación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.*

Se modifica la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en los siguientes términos:

Uno. El artículo 35.h) pasa a tener la siguiente redacción:

«h) Al acceso a la información pública, archivos y registros.»

Dos. El artículo 37 pasa a tener la siguiente redacción:

> **«Artículo 37.** *Derecho de acceso a la información pública.*
>
> Los ciudadanos tienen derecho a acceder a la información pública, archivos y registros en los términos y con las condiciones establecidas en la Constitución, en la Ley de transparencia, acceso a la información pública y buen gobierno y demás leyes que resulten de aplicación.»

Disposición final segunda. *Modificación de la Ley 5/2006, de 10 de abril, de regulación de los conflictos de intereses de los miembros del Gobierno y de los altos cargos de la Administración General del Estado.*

Se modifica la Ley 5/2006, de 10 de abril, de regulación de los conflictos de intereses de los miembros del Gobierno y de los altos cargos de la Administración General del Estado en los siguientes términos:

El apartado 4 del artículo 14 queda redactado como sigue:

> «4. El contenido de las declaraciones de bienes y derechos patrimoniales de los miembros del Gobierno y de los Secretarios de Estado y demás altos cargos previstos en el artículo 3 de esta ley se publicarán en el "Boletín Oficial del Estado", en los términos previstos reglamentariamente. En relación con los bienes patrimoniales, se publicará una declaración comprensiva de la situación patrimonial de estos altos cargos, omitiéndose aquellos datos referentes a su localización y salvaguardando la privacidad y seguridad de sus titulares.»

Disposición final tercera. *Modificación de la Ley 47/2003, de 26 de noviembre, General Presupuestaria.*

Se modifica el apartado 4 del artículo 136 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, que quedará redactado como sigue:

> «Las entidades que deban aplicar principios contables públicos, así como las restantes que no tengan obligación de publicar sus cuentas en el Registro Mercantil, publicarán anualmente en el "Boletín Oficial del Estado", el balance de situación y la cuenta del resultado económico-patrimonial, un resumen de los restantes estados que conforman las cuentas anuales y el informe de auditoría de cuentas. A estos efectos, la Intervención General de la Administración del Estado determinará el contenido mínimo de la información a publicar.»

Disposición final cuarta. *Modificación de la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.*

Se modifica el apartado 1 de la disposición adicional décima de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado, el cual quedará redactado en los siguientes términos:

> «1. La Comisión Nacional del Mercado de Valores, el Consejo de Seguridad Nuclear, las Universidades no transferidas, la Agencia Española de Protección de Datos, el Consorcio de la Zona Especial Canaria, la Comisión Nacional de los Mercados y la Competencia, el Consejo de Transparencia y Buen Gobierno, el Museo Nacional del Prado y el Museo Nacional Centro de Arte Reina Sofía se regirán por su legislación específica y supletoriamente por esta Ley.»

Disposición final quinta.

El Gobierno adoptará las medidas necesarias para optimizar el uso de los medios técnicos y humanos que se adscriban al Consejo de Transparencia y Buen Gobierno.

Disposición final sexta. *Modificación de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo.*

Se modifica la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo, en los siguientes términos:

Uno. Se añade un apartado 5 al artículo 2, con la redacción siguiente:

«5. Serán aplicables al administrador nacional del registro de derechos de emisión previsto en la Ley 1/2005, de 9 de marzo, por la que se regula el régimen de comercio de derechos de emisión de gases de efecto invernadero, con las excepciones que se determinen reglamentariamente, las obligaciones de información y de control interno contenidas en los capítulos III y IV de la presente Ley.»

Dos. Se añade un apartado 6 al artículo 7, con la redacción siguiente:

«6. Reglamentariamente podrá autorizarse la no aplicación de todas o algunas de las medidas de diligencia debida o de conservación de documentos en relación con aquellas operaciones ocasionales que no excedan de un umbral cuantitativo, bien singular, bien acumulado por periodos temporales.»

Tres. Se da nueva redacción al artículo 9, con el siguiente tenor literal:

«Artículo 9. *Medidas simplificadas de diligencia debida.*

Los sujetos obligados podrán aplicar, en los supuestos y con las condiciones que se determinen reglamentariamente, medidas simplificadas de diligencia debida respecto de aquellos clientes, productos u operaciones que comporten un riesgo reducido de blanqueo de capitales o de financiación del terrorismo.»

Cuatro. Se da nueva redacción al artículo 10, con el siguiente tenor literal:

«Artículo 10. *Aplicación de medidas simplificadas de diligencia debida.*

La aplicación de medidas simplificadas de diligencia debida será graduada en función del riesgo, con arreglo a los siguientes criterios:

a) Con carácter previo a la aplicación de medidas simplificadas de diligencia debida respecto de un determinado cliente, producto u operación de los previstos reglamentariamente, los sujetos obligados comprobarán que comporta efectivamente un riesgo reducido de blanqueo de capitales o de financiación del terrorismo.

b) La aplicación de las medidas simplificadas de diligencia debida será en todo caso congruente con el riesgo. Los sujetos obligados no aplicarán o cesarán de aplicar medidas simplificadas de diligencia debida tan pronto como aprecien que un cliente, producto u operación no comporta riesgos reducidos de blanqueo de capitales o de financiación del terrorismo.

c) Los sujetos obligados mantendrán en todo caso un seguimiento continuo suficiente para detectar operaciones susceptibles de examen especial de conformidad con lo prevenido en el artículo 17.»

Cinco. Se da nueva redacción al artículo 14, con el siguiente tenor literal:

«Artículo 14. *Personas con responsabilidad pública.*

1. Los sujetos obligados aplicarán las medidas reforzadas de diligencia debida previstas en este artículo en las relaciones de negocio u operaciones de personas con responsabilidad pública.

Se considerarán personas con responsabilidad pública las siguientes:

a) Aquellas que desempeñen o hayan desempeñado funciones públicas importantes por elección, nombramiento o investidura en otros Estados miembros de la Unión Europea o terceros países, tales como los jefes de Estado, jefes de Gobierno, ministros u otros miembros de Gobierno, secretarios de Estado o subsecretarios; los parlamentarios; los magistrados de tribunales supremos,

tribunales constitucionales u otras altas instancias judiciales cuyas decisiones no admitan normalmente recurso, salvo en circunstancias excepcionales, con inclusión de los miembros equivalentes del Ministerio Fiscal; los miembros de tribunales de cuentas o de consejos de bancos centrales; los embajadores y encargados de negocios; el alto personal militar de las Fuerzas Armadas; los miembros de los órganos de administración, de gestión o de supervisión de empresas de titularidad pública.

b) Aquellas que desempeñen o hayan desempeñado funciones públicas importantes en el Estado español, tales como los altos cargos de acuerdo con lo dispuesto en la normativa en materia de conflictos de intereses de la Administración General del Estado; los parlamentarios nacionales y del Parlamento Europeo; los magistrados del Tribunal Supremo y Tribunal Constitucional, con inclusión de los miembros equivalentes del Ministerio Fiscal; los consejeros del Tribunal de Cuentas y del Banco de España; los embajadores y encargados de negocios; el alto personal militar de las Fuerzas Armadas; y los directores, directores adjuntos y miembros del consejo de administración, o función equivalente, de una organización internacional, con inclusión de la Unión Europea.

c) Asimismo, tendrán la consideración de personas con responsabilidad pública aquellas que desempeñen o hayan desempeñado funciones públicas importantes en el ámbito autonómico español, como los Presidentes y los Consejeros y demás miembros de los Consejos de Gobierno, así como los altos cargos y los diputados autonómicos y, en el ámbito local español, los alcaldes, concejales y demás altos cargos de los municipios capitales de provincia o de capital de Comunidad Autónoma de las Entidades Locales de más de 50.000 habitantes, o cargos de alta dirección en organizaciones sindicales o empresariales o partidos políticos españoles.

Ninguna de estas categorías incluirá empleados públicos de niveles intermedios o inferiores.

2. En relación con los clientes o titulares reales que desempeñen o hayan desempeñado funciones públicas importantes por elección, nombramiento o investidura en otros Estados miembros de la Unión Europea o en un país tercero, los sujetos obligados, además de las medidas normales de diligencia debida, deberán en todo caso:

a) Aplicar procedimientos adecuados de gestión del riesgo a fin de determinar si el cliente o el titular real es una persona con responsabilidad pública. Dichos procedimientos se incluirán en la política expresa de admisión de clientes a que se refiere el artículo 26.1.

b) Obtener la autorización del inmediato nivel directivo, como mínimo, para establecer o mantener relaciones de negocios.

c) Adoptar medidas adecuadas a fin de determinar el origen del patrimonio y de los fondos.

d) Realizar un seguimiento reforzado y permanente de la relación de negocios.

3. Los sujetos obligados, además de las medidas normales de diligencia debida, deberán aplicar medidas razonables para determinar si el cliente o el titular real desempeña o ha desempeñado alguna de las funciones previstas en los párrafos b) y c) del apartado primero de este artículo.

Se entenderá por medidas razonables la revisión, de acuerdo a los factores de riesgo presentes en cada caso, de la información obtenida en el proceso de diligencia debida.

En el caso de relaciones de negocio de riesgo más elevado, los sujetos obligados aplicarán las medidas previstas en los párrafos b), c) y d) del apartado precedente.

4. Los sujetos obligados aplicarán las medidas establecidas en los dos apartados anteriores a los familiares y allegados de las personas con responsabilidad pública.

A los efectos de este artículo tendrá la consideración de familiar el cónyuge o la persona ligada de forma estable por análoga relación de afectividad, así como los padres e hijos, y los cónyuges o personas ligadas a los hijos de forma estable por análoga relación de afectividad.

Se considerará allegado toda persona física de la que sea notorio que ostente la titularidad o el control de un instrumento o persona jurídicos conjuntamente con una persona con responsabilidad pública, o que mantenga otro tipo de relaciones empresariales estrechas con la misma, o que ostente la titularidad o el control de un instrumento o persona jurídicos que notoriamente se haya constituido en beneficio de la misma.

5. Los sujetos obligados aplicarán medidas razonables para determinar si el beneficiario de una póliza de seguro de vida y, en su caso, el titular real del beneficiario, es una persona con responsabilidad pública con carácter previo al pago de la prestación derivada del contrato o al ejercicio de los derechos de rescate, anticipo o pignoración conferidos por la póliza.

En el caso de identificar riesgos más elevados, los sujetos obligados, además de las medidas normales de diligencia debida, deberán:

a) Informar al inmediato nivel directivo, como mínimo, antes de proceder al pago, rescate, anticipo o pignoración.

b) Realizar un escrutinio reforzado de la entera relación de negocios con el titular de la póliza.

c) Realizar el examen especial previsto en el artículo 17 a efectos de determinar si procede la comunicación por indicio de conformidad con el artículo 18.

6. Sin perjuicio del cumplimiento de lo establecido en los apartados anteriores, cuando, por concurrir las circunstancias previstas en el artículo 17, proceda el examen especial, los sujetos obligados adoptarán las medidas adecuadas para apreciar la eventual participación en el hecho u operación de quien ostente o haya ostentado en España la condición de cargo público representativo o alto cargo de las Administraciones Públicas, o de sus familiares o allegados.

7. Sin perjuicio de lo dispuesto en el artículo 11, cuando las personas contempladas en los apartados precedentes hayan dejado de desempeñar sus funciones, los sujetos obligados continuarán aplicando las medidas previstas en este artículo por un periodo de dos años.»

Seis. Se da nueva redacción al apartado 4 del artículo 26, con el siguiente tenor literal:

«4. Las medidas de control interno se establecerán a nivel de grupo, con las especificaciones que se determinen reglamentariamente. A efectos de la definición de grupo, se estará a lo dispuesto en el artículo 42 del Código de Comercio.»

Siete. Se da nueva redacción al artículo 42, con el siguiente tenor literal:

«Artículo 42. *Sanciones y contramedidas financieras internacionales.*

1. Las sanciones financieras establecidas por las Resoluciones del Consejo de Seguridad de Naciones Unidas relativas a la prevención y supresión del terrorismo y de la financiación del terrorismo, y a la prevención, supresión y disrupción de la proliferación de armas de destrucción masiva y de su financiación, serán de obligada aplicación para cualquier persona física o jurídica en los términos previstos por los reglamentos comunitarios o por acuerdo del Consejo de Ministros, adoptado a propuesta del Ministro de Economía y Competitividad.

2. Sin perjuicio del efecto directo de los reglamentos comunitarios, el Consejo de Ministros, a propuesta del Ministro de Economía y Competitividad, podrá acordar la aplicación de contramedidas financieras respecto de países terceros que supongan riesgos más elevados de blanqueo de capitales, financiación del terrorismo o financiación de la proliferación de armas de destrucción masiva.

El acuerdo de Consejo de Ministros, que podrá adoptarse de forma autónoma o en aplicación de decisiones o recomendaciones de organizaciones, instituciones o grupos internacionales, podrá imponer, entre otras, las siguientes contramedidas financieras:

a) Prohibir, limitar o condicionar los movimientos de capitales y sus correspondientes operaciones de cobro o pago, así como las transferencias, de o hacia el país tercero o de nacionales o residentes del mismo.

b) Someter a autorización previa los movimientos de capitales y sus correspondientes operaciones de cobro o pago, así como las transferencias, de o hacia el país tercero o de nacionales o residentes del mismo.

c) Acordar la congelación o bloqueo de los fondos y recursos económicos cuya propiedad, tenencia o control corresponda a personas físicas o jurídicas nacionales o residentes del país tercero.

d) Prohibir la puesta a disposición de fondos o recursos económicos cuya propiedad, tenencia o control corresponda a personas físicas o jurídicas nacionales o residentes del país tercero.

e) Requerir la aplicación de medidas reforzadas de diligencia debida en las relaciones de negocio u operaciones de nacionales o residentes del país tercero.

f) Establecer la comunicación sistemática de las operaciones de nacionales o residentes del país tercero o que supongan movimientos financieros de o hacia el país tercero.

g) Prohibir, limitar o condicionar el establecimiento o mantenimiento de filiales, sucursales u oficinas de representación de las entidades financieras del país tercero.

h) Prohibir, limitar o condicionar a las entidades financieras el establecimiento o mantenimiento de filiales, sucursales u oficinas de representación en el país tercero.

i) Prohibir, limitar o condicionar las relaciones de negocio o las operaciones financieras con el país tercero o con nacionales o residentes del mismo.

j) Prohibir a los sujetos obligados la aceptación de las medidas de diligencia debida practicadas por entidades situadas en el país tercero.

k) Requerir a las entidades financieras la revisión, modificación y, en su caso, terminación, de las relaciones de corresponsalía con entidades financieras del país tercero.

l) Someter las filiales o sucursales de entidades financieras del país tercero a supervisión reforzada o a examen o auditoría externos.

m) Imponer a los grupos financieros requisitos reforzados de información o auditoría externa respecto de cualquier filial o sucursal localizada o que opere en el país tercero.

3. Competerá al Servicio Ejecutivo de la Comisión la supervisión e inspección del cumplimiento de lo dispuesto en este artículo.»

Ocho. Se da nueva redacción al artículo 52.1.u), con el siguiente tenor literal:

«u) El incumplimiento de la obligación de aplicar sanciones o contramedidas financieras internacionales, en los términos del artículo 42.»

Disposición final séptima. *Desarrollo reglamentario.*

El Gobierno, en el ámbito de sus competencias, podrá dictar cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta Ley.

El Consejo de Ministros aprobará, en el plazo de tres meses desde la publicación de esta Ley en el «Boletín Oficial del Estado», un Real Decreto por el que se apruebe el Estatuto orgánico del Consejo de Transparencia y Buen Gobierno.

Disposición final octava. *Título competencial.*

La presente Ley se dicta al amparo de lo dispuesto en los artículos 149.1.1.ª, 149.1.13.ª y 149.1.18.ª de la Constitución. Se exceptúa lo dispuesto en el segundo párrafo del apartado 2 del artículo 6, el artículo 9, los apartados 1 y 2 del artículo 10, el artículo 11, el apartado 2 del artículo 21, el apartado 1 del artículo 25, el título III y la disposición adicional segunda.

Disposición final novena. *Entrada en vigor.*

La entrada en vigor de esta ley se producirá de acuerdo con las siguientes reglas:

– Las disposiciones previstas en el título II entrarán en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».

– El título preliminar, el título I y el título III entrarán en vigor al año de su publicación en el «Boletín Oficial del Estado».

– Los órganos de las Comunidades Autónomas y Entidades Locales dispondrán de un plazo máximo de dos años para adaptarse a las obligaciones contenidas en esta Ley.

Información relacionada

- Véanse los Reales Decretos 415/2016, de 3 de noviembre, Ref. BOE-A-2016-10167, 424/2016, de 11 de noviembre, Ref. BOE-A-2016-10459 y 769/2017, de 28 de julio, Ref. BOE-A-2017-9012, por los que el Portal de la Transparencia pasa a depender del Ministerio de Hacienda y Función Pública.

§ 55

Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público

Jefatura del Estado
«BOE» núm. 276, de 17 de noviembre de 2007
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2007-19814

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

La información generada desde las instancias públicas, con la potencialidad que le otorga el desarrollo de la sociedad de la información, posee un gran interés para las empresas a la hora de operar en sus ámbitos de actuación, contribuir al crecimiento económico y la creación de empleo, y para los ciudadanos como elemento de transparencia y guía para la participación democrática. Recogiendo ambas aspiraciones la Directiva 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público, se adoptó con la finalidad de explotar el potencial de información del sector público y superar las barreras de un mercado europeo fragmentado estableciendo unos criterios homogéneos, asentados en condiciones equitativas, proporcionadas y no discriminatorias para el tratamiento de la información susceptible de ser reutilizada por personas físicas o jurídicas.

Las diferentes Administraciones y organismos del sector público recogen, producen, reproducen y difunden documentos para llevar a cabo la misión de servicio público que tienen encomendada. Como expresa la Directiva 2003/98/CE, la utilización de dichos documentos por otros motivos, ya sea con fines comerciales o no comerciales, constituye una reutilización. Por una parte, se persigue armonizar la explotación de la información en el sector público, en especial la información en soporte digital recopilada por sus distintos organismos relativa a numerosos ámbitos de interés como la información social, económica, jurídica, geográfica, meteorológica, turística, sobre empresas, patentes y educación, etc., al objeto de facilitar la creación de productos y servicios de información basados en documentos del sector público, y reforzar la eficacia del uso transfronterizo de estos documentos por parte de los ciudadanos y de las empresas privadas para que ofrezcan productos y servicios de información de valor añadido. Por otra parte, la publicidad de todos los documentos de libre disposición que obran en poder del sector público referentes no sólo

a los procedimientos políticos, sino también a los judiciales, económicos y administrativos, es un instrumento esencial para el desarrollo del derecho al conocimiento, que constituye un principio básico de la democracia.

Estos objetivos son los que persigue la presente ley, que mediante la incorporación a nuestro ordenamiento jurídico de la Directiva 2003/98/CE y, tomando como punto de partida el diverso tratamiento que las Administraciones y organismos del sector público han otorgado a la explotación de la información, dispone un marco general mínimo para las condiciones de reutilización de los documentos del sector público que acoja las diferentes modalidades que se pueden adoptar y que dimanan de la heterogeneidad de la propia información. En consecuencia, se prevé que sean las Administraciones y organismos del sector público los que decidan autorizar o no la reutilización de los documentos o categorías de documentos por ellos conservados con fines comerciales o no comerciales. Asimismo, se pretende promover la puesta a disposición de los documentos por medios electrónicos, propiciando el desarrollo de la sociedad de la información.

La ley posee unos contornos específicos que la delimitan del régimen general de acceso previsto en el artículo 105 b) de la Constitución Española y en su desarrollo legislativo, en esencia representado por la Ley 30/1992, de 26 de noviembre, del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En este sentido resulta necesario precisar que no se modifica el régimen de acceso a los documentos administrativos consagrado en nuestro ordenamiento jurídico, sino que se aporta un valor añadido al derecho de acceso, contemplando el marco de regulación básico para la explotación de la información que obra en poder del sector público, en un marco de libre competencia, regulando las condiciones mínimas a las que debe acogerse un segundo nivel de tratamiento de la información que se genera desde las instancias públicas.

En el Título I de la ley se prevé el ámbito subjetivo de aplicación, que se extiende a las Administraciones y organismos del sector público en el sentido definido en su artículo 2, en consonancia con la delimitación realizada en la normativa de contratación del sector público. Desde la perspectiva de su aplicación objetiva, la ley contempla una definición genérica del término documento, acorde con la evolución de la sociedad de la información y que engloba todas las formas de representación de actos, hechos o información, y cualquier recopilación de los mismos, independientemente del soporte (escrito en papel, almacenado en forma electrónica o como grabación sonora, visual o audiovisual) conservados por las Administraciones y organismos del sector público, e incluye una delimitación negativa del ámbito de aplicación, enumerando aquellos documentos o categorías de documentos que no se encuentran afectados por la misma, atendiendo a diversos criterios. En este punto cabe precisar que la ley no se aplica a los documentos sometidos a derechos de propiedad intelectual o industrial (como las patentes, los diseños y las marcas registradas) especialmente por parte de terceros. A los efectos de esta ley se entiende por derechos de propiedad intelectual los derechos de autor y derechos afines, incluidas las formas de protección sui géneris. En este sentido, la ley tampoco afecta a la existencia de derechos de propiedad intelectual de las Administraciones y organismos del sector público, ni restringe en modo alguno el ejercicio de esos derechos fuera de los límites establecidos en su articulado. Las obligaciones impuestas por esta ley sólo deben aplicarse en la medida en que resulten compatibles con las disposiciones de los acuerdos internacionales sobre protección de los derechos de propiedad intelectual, en particular el Convenio de Berna para la protección de las obras literarias y artísticas (Convenio de Berna) y el Acuerdo sobre aspectos de los derechos de propiedad intelectual relacionados con el comercio (Acuerdo ADPIC). No obstante, las instancias públicas deben ejercer sus derechos de autor de una manera que facilite la reutilización.

El Título II prevé los aspectos básicos del régimen jurídico de la reutilización, indicando que las Administraciones y organismos del sector público podrán optar por permitir la reutilización sin condiciones concretas o, mediante la expedición de una licencia, que imponga a su titular una serie de condiciones de reutilización que, en todo caso, deberán ser claras, justas y transparentes, no discriminatorias para categorías comparables de reutilización y atender al principio de libre competencia y de servicio público.

Para ello el uso de licencias-tipo que puedan estar disponibles por medios electrónicos se revela como un elemento clave en este sentido. Por otra parte, se prevé que las distintas

Administraciones y organismos difundan qué documentación es susceptible de ser reutilizada mediante la creación de listados e índices accesibles en línea de los documentos disponibles, con el objeto de fomentar y facilitar las solicitudes de reutilización. Para incrementar las posibilidades de reutilización, las Administraciones y organismos del sector público deben procurar ofrecer los documentos por medios electrónicos en los formatos o lenguas preexistentes.

El régimen de reutilización garantiza el pleno respeto de los principios que consagran la protección de datos personales, en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y su normativa de desarrollo.

Por otra parte, las Administraciones y organismos del sector público deben adecuarse a las normas de competencia, evitando acuerdos exclusivos. No obstante, la ley prevé una excepción a este principio cuando, con vistas a la prestación de un servicio de interés económico general, pueda resultar necesario conceder un derecho exclusivo a la reutilización de determinados documentos del sector público.

Asimismo, la ley prevé los principios aplicables para aquellos supuestos en los que las Administraciones y organismos exijan contraprestaciones económicas por facilitar la reutilización de documentos con fines comerciales, cuya cuantía deberá ser razonable y orientada al coste, sin que los ingresos obtenidos superen los costes totales de recogida, producción, reproducción y difusión de los documentos.

En el Título II se concretan algunos aspectos de la reutilización de la información, previendo las posibles condiciones a las que someter la reutilización, que podrían ir referidas a cuestiones como el uso correcto de los documentos, la garantía de que los documentos no serán modificados y la indicación de la fuente. Asimismo se indica el contenido mínimo que deben acoger las licencias.

En el Título III la ley establece el procedimiento para poder arbitrar las solicitudes de reutilización, en el que tienen una especial relevancia los plazos de resolución, aspecto esencial para el contenido dinámico de la información, cuyo valor económico depende de su puesta a disposición inmediata y de una actualización regular. Asimismo se garantiza que en las resoluciones que se adopten se indiquen las vías de recurso de las que disponen los solicitantes para impugnar las decisiones que les afecten.

Por último se establece para la Administración General del Estado un régimen sancionador conectado con el mal uso que se confiera a la información cuya reutilización ha sido autorizada.

La presente Ley tiene carácter de legislación básica al amparo de lo dispuesto en el artículo 149.1.18.ª de la Constitución. Se exceptúa el artículo 11 y los apartados 1 (párrafos segundo y tercero), 3 y 8 del artículo 10.

En la elaboración de la ley se ha recabado el informe de la Agencia Española de Protección de Datos.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente ley tiene por objeto la regulación básica del régimen jurídico aplicable a la reutilización de los documentos elaborados o custodiados por los sujetos incluidos en el ámbito subjetivo de aplicación regulado en el artículo 2, así como de los datos de investigación de acuerdo con las condiciones establecidas en el artículo 3.bis.

La aplicación de esta ley se hará sin perjuicio del régimen aplicable al derecho de acceso a los documentos y a las especialidades previstas en su normativa reguladora.

Artículo 2. *Ámbito subjetivo de aplicación.*

La presente Ley se aplica a:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local.

b) Los organismos y entidades del sector público institucional creados para satisfacer necesidades de interés general, que no tengan carácter industrial o mercantil.

c) Las sociedades mercantiles pertenecientes al sector público institucional que:

1.º Lleven a cabo su actividad en los ámbitos definidos en la Directiva 2014/25/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales y por la que se deroga la Directiva 2004/17/CE Texto pertinente a efectos del EEE.

2.º Actúen como operadores de servicio público con arreglo al artículo 2 del Reglamento (CE) n.º 1370/2007 del Parlamento Europeo y del Consejo, de 23 de octubre de 2007, sobre los servicios públicos de transporte de viajeros por ferrocarril y carretera y por el que se derogan los Reglamentos (CEE) n.º 1191/69 y (CEE) n.º 1107/70 del Consejo.

3.º Actúen como compañías aéreas que cumplen obligaciones de servicio público con arreglo al artículo 16 del Reglamento (CE) n.º 1008/2008 del Parlamento Europeo y del Consejo, de 24 de septiembre de 2008, sobre normas comunes para la explotación de servicios aéreos en la Comunidad.

4.º Actúen como armadores comunitarios que cumplen obligaciones de servicio público con arreglo al artículo 4 del Reglamento (CEE) n.º 3577/92 del Consejo, de 7 de diciembre de 1992, por el que se aplica el principio de libre prestación de servicios a los transportes marítimos dentro de los Estados miembros (cabotaje marítimo).

Artículo 3. *Ámbito objetivo de aplicación.*

1. Se entiende por reutilización el uso por personas físicas o jurídicas de documentos elaborados o custodiados por:

a) Los sujetos previstos en los párrafos a) y b) del artículo 2, con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos en la actividad de servicio público para la que se produjeron, excepto para el intercambio de documentos entre dichos sujetos en el marco de sus actividades de servicio público.

b) Las sociedades mercantiles públicas a que se refiere el párrafo c) del artículo 2 con fines comerciales o no comerciales distintos del propósito inicial que tenían esos documentos de prestar servicios de interés general para el que se produjeron, excepto para el intercambio de documentos entre estas sociedades mercantiles públicas y el resto de sujetos previstos en el artículo 2 que se realice exclusivamente en el desarrollo de las actividades de servicio público de estos últimos.

2. Esta ley se aplica, asimismo, a los datos de investigación en los términos previstos en el artículo 3.bis y a los documentos a los que se aplica la Directiva 2007/2/CE del Parlamento Europeo y del Consejo, de 14 de marzo de 2007, por la que se establece una infraestructura de información espacial en la Comunidad Europea (Inspire).

3. Esta ley no será aplicable a los siguientes documentos elaborados o custodiados por los sujetos previstos en el artículo 2:

a) Los documentos sobre los que existan prohibiciones o limitaciones en el derecho de acceso en virtud de lo previsto en el artículo 13 de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y las demás normas que regulan el derecho de acceso o la publicidad registral con carácter específico.

b) De conformidad con su legislación específica, los documentos que afecten a la defensa nacional, la seguridad del Estado, la protección de la seguridad pública, así como los obtenidos por la Administración Tributaria y la Administración de la Seguridad Social en el desempeño de sus funciones, los sometidos al secreto estadístico, a la confidencialidad comercial, tales como secretos comerciales, profesionales o empresariales y, en general, los documentos relacionados con actuaciones sometidas por una norma al deber de reserva, secreto o confidencialidad.

c) Los documentos para cuyo acceso se requiera ser titular de un derecho o interés legítimo.

d) Los documentos que obran en poder de los sujetos previstos en los párrafos a) y b) del artículo 2 para finalidades ajenas a las funciones de servicio público de acuerdo con la legislación aplicable y en particular, con la normativa de creación del servicio público de que se trate.

e) Los documentos sobre los que existan derechos de propiedad intelectual o industrial por parte de terceros.

No obstante, esta ley no afecta a la existencia de derechos de propiedad intelectual de los sujetos previstos en el artículo 2 ni a su posesión por éstos, ni restringe el ejercicio de esos derechos fuera de los límites establecidos por esta ley. El ejercicio de los derechos de propiedad intelectual de los sujetos previstos en el artículo 2 deberá realizarse de forma que se facilite su reutilización.

Lo previsto en el párrafo anterior será de aplicación, asimismo, a los documentos respecto de los que las bibliotecas, incluidas las universitarias, los museos y los archivos sean titulares originarios de los derechos de propiedad intelectual como creadores de la misma conforme a lo establecido en la legislación de propiedad intelectual, así como cuando sean titulares porque se les haya transmitido la titularidad de los derechos sobre dicha obra según lo dispuesto en la citada legislación, debiendo en este caso respetar lo establecido en los términos de la cesión.

f) Los documentos conservados por las entidades que gestionen los servicios esenciales de radiodifusión sonora y televisiva y sus filiales.

g) Los documentos conservados por instituciones educativas de nivel secundario e inferior y, en el caso de todas las demás instituciones educativas, documentos distintos de los datos investigación referidos en el artículo 1.

h) Los documentos distintos de los datos de investigación mencionados en el artículo 1, conservados por organizaciones que realizan actividades de investigación y organizaciones que financian la investigación, incluidas las organizaciones creadas para la transferencia de los resultados de la investigación.

i) Los documentos producidos o conservados por instituciones culturales que no sean bibliotecas, incluidas las universitarias, museos y archivos.

j) Los logotipos, divisas e insignias.

k) Los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de los datos personales, de conformidad con la normativa vigente y las partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización se haya definido por ley como incompatible con la legislación relativa a la protección de las personas físicas con respecto al tratamiento de los datos personales.

l) Los documentos elaborados por entidades del sector público empresarial, excepto las previstas en el párrafo c) del artículo 2, y fundacional en el ejercicio de las funciones atribuidas legalmente y los de carácter comercial, industrial o mercantil elaborado en ejecución del objeto social previsto en sus Estatutos.

m) Los estudios realizados por entidades del sector público en colaboración con el sector privado, mediante convenios o cualquier otro tipo de instrumento, como fórmula de financiación de los mismos.

n) Los documentos cuyo acceso esté excluido o limitado por motivos de protección de información sensible sobre infraestructuras críticas.

ñ) Los documentos producidos o conservados por las sociedades mercantiles públicas previstas en el párrafo c) del artículo 2, fuera del ámbito de la prestación de servicios de interés general o relativos a actividades sometidas directamente a la competencia y no sujetas a la normativa de contratación de entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales.

4. En ningún caso, podrá ser objeto de reutilización, la información en que la ponderación a la que se refieren los artículos 5.3 y 15 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, arroje como resultado la prevalencia del derecho fundamental a la protección de datos de carácter personal, a menos que se produzca la disociación de los datos a la que se refiere el artículo 15.4 de la citada Ley.

Artículo 3.bis. *Datos de investigación.*

1. Las entidades incluidas en el ámbito de aplicación del artículo 2 de la presente Ley y que realicen actividades de investigación o financien la investigación adoptarán medidas para apoyar que los datos de investigaciones financiadas públicamente sean plenamente reutilizables, interoperables y de acceso abierto, teniendo en cuenta las limitaciones que pudieran derivarse de los derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos.

2. Sin perjuicio de lo previsto en el artículo 3.3.e) y de los intereses comerciales legítimos, las actividades de transferencia de conocimientos y los derechos de propiedad intelectual preexistentes, los datos de investigación serán reutilizables para fines comerciales o no comerciales, de conformidad con lo dispuesto en la presente Ley, cuando sean financiados con fondos públicos y cuando los investigadores, las universidades o las organizaciones que realizan actividades de investigación o que financien la investigación ya hubieran puesto tales datos a disposición del público a través de un repositorio institucional o temático y, en todo caso, con pleno respeto a la normativa vigente en materia de propiedad intelectual.

Artículo 3.ter. *Conjuntos de datos de alto valor.*

1. Además de la lista de conjuntos de datos específicos de alto valor que, en su caso, establezca la Comisión Europea, se podrán determinar a nivel nacional otros conjuntos de datos adicionales seleccionados en relación a su potencial para generar beneficios socioeconómicos o medioambientales importantes y servicios innovadores; beneficiar a un gran número de usuarios, en concreto pymes; contribuir a generar ingresos, y la posibilidad de ser combinados con otros conjuntos de datos.

2. Dichos conjuntos de datos de alto valor, tanto los establecidos a nivel europeo como nacional:

a) Estarán disponibles gratuitamente, a reserva de lo previsto en el artículo 7.9.a).
b) Serán legibles por máquina
c) Se suministrarán a través de interfaz de programación de aplicaciones (API), y
d) Se proporcionarán en forma de descarga masiva, cuando proceda.

Se podrán especificar acuerdos organizativos relativos a la publicación y de reutilización de los tipos de conjuntos de datos de alto valor. Esos acuerdos serán compatibles con las licencias tipo abiertas. Los acuerdos podrán incluir condiciones aplicables a la reutilización, el formato de los datos y los metadatos, así como acuerdos técnicos para la difusión.

3. El Ministerio de Asuntos Económicos y Transformación Digital aprobará la lista de los conjuntos de datos de alto valor nacionales que se publicará mediante Resolución de la Secretaria de Estado de Digitalización e Inteligencia Artificial. La selección y actualización de los conjuntos de datos incluidos en dicha lista se realizará a través de la División Oficina del Dato contando con la colaboración de los actores interesados, tanto públicos como privados, a través de los órganos y mecanismos que se establezcan.

TÍTULO II

Régimen jurídico de la reutilización

Artículo 4. *Régimen administrativo de la reutilización.*

1. Los documentos de los sujetos previstos en el artículo 2 serán reutilizables en los términos previstos en esta ley. Dichos sujetos velarán porque los documentos a los que se aplica esta normativa puedan ser reutilizados para fines comerciales o no comerciales de conformidad con alguna o algunas de las siguientes modalidades:

a) Reutilización de documentos puestos a disposición del público sin sujeción a condiciones.

b) Reutilización de documentos puestos a disposición del público con sujeción a condiciones establecidas en licencias-tipo.

c) Reutilización de documentos previa solicitud, conforme al procedimiento previsto en el artículo 10 o, en su caso, en la normativa autonómica, pudiendo incorporar en estos supuestos condiciones establecidas en una licencia.

d) Acuerdos exclusivos conforme el procedimiento previsto en el artículo 6.

2. La reutilización de documentos no estará sujeta a condiciones a menos que estas sean objetivas, proporcionadas, no discriminatorias y estén justificadas por un objetivo de interés público. En los supuestos de sujeción, las condiciones se fijarán en una licencia.

Los sujetos previstos en el artículo 2 podrán facilitar licencias-tipo para la reutilización de documentos, las cuales deberán estar disponibles en formato digital y ser procesables electrónicamente.

3. Las condiciones incorporadas en las licencias habrán de respetar los siguientes criterios:

a) Deberán ser claras, justas y transparentes.

b) No deberán restringir las posibilidades de reutilización ni limitar la competencia.

c) No deberán ser discriminatorias para categorías comparables de reutilización, incluida la reutilización transfronteriza.

4. Los sujetos a que se refieren los párrafos a) y b) del artículo 2 no ejercerán el derecho del fabricante de una base de datos previsto en el artículo 133 de la Ley 5/1998, de 6 de marzo, de incorporación al Derecho español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, sobre la protección jurídica de las bases de datos, para evitar la reutilización de documentos o restringir la reutilización más allá de los límites establecidos en esta Ley.

5. Los sujetos previstos en el artículo 2 crearán dispositivos y sistemas de gestión documental que permitan a los ciudadanos una recuperación eficaz de la información, disponible en línea y que enlacen con los dispositivos y sistemas de gestión puestos a disposición por otras Administraciones. Asimismo, facilitarán herramientas informáticas que permitan el acceso en línea a los listados de los documentos que puedan ser ampliamente reutilizables y la búsqueda de los documentos disponibles para su reutilización, con los metadatos pertinentes de conformidad con lo establecido en las normas técnicas de interoperabilidad, accesibles, siempre que sea posible y apropiado, en línea y en formato legible por máquina.

Los sujetos previstos en los párrafos a) y b) del artículo 2 promoverán la creación de sistemas que permitan la conservación de los documentos disponibles para su reutilización.

La Administración General del Estado mantendrá el catálogo nacional de información pública reutilizable en el que se pondrán a disposición los conjuntos de datos relativos a los documentos a los que aplica la presente Ley, en formatos accesibles, fáciles de localizar y reutilizables. Este catálogo dará cobertura, al menos, al ámbito de la Administración General del Estado y a sus organismos y entidades de derecho público vinculados o dependientes. Los posibles catálogos de información pública reutilizable establecidos por el resto de sujetos previstos en el artículo 2 deberán interoperar con el catálogo nacional cumpliendo las Normas Técnicas de Interoperabilidad que se establezcan al respecto.

Los catálogos de información pública reutilizable proporcionarán información sobre los derechos previstos en esta ley y ofrecerán la ayuda pertinente.

En la medida de lo posible, se facilitará la búsqueda multilingüe de los documentos, en particular permitiendo la agregación de metadatos a escala de la Unión Europea.

6. La reutilización de documentos que contengan datos de carácter personal se regirá por lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

7. La utilización de los conjuntos de datos se realizará por parte de los usuarios o agentes de la reutilización bajo su responsabilidad y riesgo, correspondiéndoles en exclusiva a ellos responder frente a terceros por daños que pudieran derivarse de ella.

Los sujetos previstos en el artículo 2 no serán responsables del uso que de su información hagan los agentes reutilizadores ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos, provocados por el uso de la información reutilizada.

8. La puesta a disposición de un documento para su reutilización no supone renuncia al derecho a su explotación, ni es impedimento para la modificación de los datos que en el mismo consten como consecuencia del ejercicio de funciones o competencias de dicho sujeto.

9. Igualmente, no se podrá indicar, de ningún modo, que los sujetos previstos en el artículo 2 pertenecientes al ámbito estatal titulares de la información reutilizada participan, patrocinan o apoyan la reutilización que se lleve a cabo de ella.

Artículo 5. *Formatos disponibles para la reutilización.*

1. La elaboración y la puesta a disposición de los documentos incluidos en el ámbito de aplicación de la presente Ley se efectuará, en la medida de lo posible, conforme al principio de documentos abiertos desde el diseño y por defecto.

2. Los sujetos previstos en el artículo 2 promoverán que la puesta a disposición de los documentos para su reutilización, así como que la tramitación de solicitudes de reutilización se realice por medios electrónicos y mediante plataforma multicanal cuando ello sea compatible con los medios técnicos de que disponen.

3. Los sujetos previstos en el artículo 2 facilitarán sus documentos en cualquier formato o lengua preexistente, pero también procurarán, siempre que ello sea posible y apropiado, proporcionarlos en formato abierto, accesible, legible por máquina conforme a lo previsto en el apartado anterior y conjuntamente con sus metadatos, con los niveles más elevados de precisión y desagregación, fáciles de localizar y reutilizables. Tanto el formato como los metadatos, en la medida de lo posible, deben cumplir estándares y normas formales abiertas. Esto no implicará que estén obligados a crear documentos, adaptarlos o facilitar extractos de documentos, cuando ello suponga un esfuerzo desproporcionado que conlleve algo más que una simple manipulación.

4. Los sujetos previstos en el artículo 2 pondrán a disposición los datos dinámicos de los que dispongan para su reutilización inmediatamente después de su recopilación, a través de interfaces de programación de aplicaciones (API) adecuadas y, cuando proceda, en forma de descarga masiva.

Cuando la puesta a disposición de datos dinámicos para su reutilización inmediatamente después de su recopilación pueda superar sus capacidades financieras o técnicas suponiendo un esfuerzo desproporcionado, esos datos dinámicos se pondrán a disposición para su reutilización en un plazo o con restricciones técnicas temporales que no perjudiquen indebidamente su potencial económico y social.

5. Los conjuntos de datos de alto valor, conforme al artículo 3 ter, que obren en poder de los sujetos previstos en el artículo 2 se pondrán a disposición para su reutilización en un formato legible por máquina, a través de interfaces de programación de aplicaciones adecuadas y, cuando proceda, en forma de descarga masiva.

6. Con arreglo a la presente Ley, no podrá exigirse a los sujetos previstos en el artículo 2 que mantengan la producción y el almacenamiento de un determinado tipo de documento con vistas a su reutilización.

7. Sin perjuicio de las definiciones establecidas en el Anexo, la puesta a disposición de los documentos para su reutilización por medios electrónicos por parte de los sujetos previstos en el artículo 2 debe realizarse en los términos establecidos por las normas reguladoras de la Administración electrónica, la interoperabilidad y los datos abiertos.

8. Con arreglo a lo establecido en el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por el Real Decreto Legislativo 1/2013, de 29 de noviembre, los medios electrónicos de puesta a disposición de los documentos a que se refiere el apartado 2 de este artículo serán accesibles a las personas con discapacidad, de acuerdo con las normas técnicas existentes en la materia.

Asimismo, los sujetos previstos en el artículo 2 adoptarán, en lo posible, las medidas adecuadas para facilitar que aquellos documentos destinados a personas con discapacidad estén disponibles en formatos que tengan en cuenta las posibilidades de reutilización por parte de dichas personas.

No regirá esta obligación en los supuestos en los que dicha adecuación no constituya un ajuste razonable, entendiéndose por tal lo dispuesto en el artículo 7 del texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social.

Artículo 6. *Prohibición de derechos exclusivos.*

1. La reutilización de documentos estará abierta a todos los agentes potenciales del mercado, incluso en caso de que uno o más de los agentes exploten ya productos con valor añadido basados en estos documentos.

Los contratos o acuerdos de otro tipo entre los sujetos previstos en el artículo 2 que conserven los documentos y los terceros no otorgarán derechos exclusivos, sin perjuicio de lo previsto en los siguientes apartados.

2. Solo será admisible la suscripción de acuerdos exclusivos que corresponda a los mencionados sujetos a favor de terceros cuando tales derechos exclusivos sean necesarios para la prestación de un servicio de interés público. En tal caso, el sujeto previsto en el artículo 2 de que se trate quedará obligado a la realización de una revisión periódica, y en todo caso, cada tres años, con el fin de determinar si permanece la causa que justificó la concesión del mencionado derecho exclusivo. Estos acuerdos exclusivos deberán ser transparentes y públicos, debiendo ser puestos a disposición del público en línea al menos dos meses antes de su entrada en vigor.

3. Excepcionalmente, cuando exista un acuerdo exclusivo relacionado con la digitalización de los recursos culturales, el período de exclusividad no será superior, por regla general, a diez años. En el caso de que lo sea, su duración se revisará durante el undécimo año y, si procede, cada siete años a partir de entonces. Tales acuerdos deberán ser transparentes y se pondrán en conocimiento del público.

Cuando exista un acuerdo exclusivo en el sentido establecido en el párrafo anterior deberá facilitarse gratuitamente al sujeto de que se trate previsto en los párrafos a) y b) del artículo 2, como parte de dichos acuerdos, una copia de los recursos culturales digitalizados de la misma calidad y características técnicas del original, tales como formato, resolución, gama de colores, etc., con sus metadatos y requisitos técnicos de digitalización establecidos en la normas nacionales e internacionales pertinentes. Esa copia estará disponible para su reutilización una vez finalizado el período de exclusividad.

4. Los acuerdos que, sin conceder expresamente un derecho exclusivo, conlleven una disponibilidad limitada para la reutilización de documentos por entidades distintas de quienes participen en el acuerdo, deberán ser transparentes y públicos, siendo sus condiciones finales puestas a disposición del público en línea al menos dos meses antes de su entrada en vigor. El efecto de estos acuerdos sobre la disponibilidad de datos para su reutilización estará sujeto a revisiones periódicas y, en todo caso, se someterá a revisión cada tres años.

Artículo 7. *Tarifas.*

1. La reutilización de los documentos será gratuita. No obstante, podrá aplicarse una tarifa por el suministro de documentos para su reutilización en las condiciones previstas en la normativa estatal vigente o, en su caso, en la normativa que resulte de aplicación en el ámbito autonómico o local, limitándose la misma a los costes marginales en que se incurra para su reproducción, puesta a disposición, difusión, anonimización de datos personales y las medidas adoptadas para proteger información comercial confidencial.

En caso de que un sujeto previsto en el artículo 2 reutilice los documentos como base para actividades comerciales ajenas a las funciones propias que tenga atribuidas, deberán aplicarse a la entrega de documentos para dichas actividades las mismas tarifas y condiciones que se apliquen a los demás usuarios.

2. Lo dispuesto en el apartado anterior no se aplicará a:

a) Los sujetos previstos en el párrafo b) del artículo 2 a los que se exija generar ingresos para cubrir una parte sustancial de sus costes relativos a la realización de sus misiones de servicio público.

b) Las bibliotecas, incluidas las universitarias, los museos y los archivos.

c) Las sociedades mercantiles públicas a que se refiere párrafo c) del artículo 2.

3. Se publicará en línea una lista de los sujetos a los que se refiere la letra a) del apartado anterior.

4. En los casos a los que se refieren los párrafos a) y c) del apartado 2, se calculará el precio total conforme a criterios objetivos, transparentes y comprobables, que serán fijados mediante la normativa que corresponda. Los ingresos totales de cada sujeto obtenidos por

suministrar documentos y autorizar su reutilización durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción, difusión y almacenamiento de datos, incrementado por un margen de beneficio razonable de la inversión y, en su caso, anonimización de datos personales y medidas adoptadas para proteger la información comercial confidencial. La tarifa se calculará conforme a los principios contables aplicables y de acuerdo con la normativa aplicable.

5. Cuando quienes apliquen tarifas sean los sujetos mencionados en el párrafo b) del apartado 2, los ingresos totales obtenidos por suministrar y autorizar la reutilización de documentos durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción, difusión, almacenamiento de datos, conservación, compensación de derechos y, en su caso, anonimización de datos personales y medidas adoptadas para proteger la información comercial confidencial, incrementado por un margen de beneficio razonable de la inversión. A efectos de calcular dicho margen, estos sujetos podrán tener en cuenta los precios aplicados por el sector privado por la reutilización de documentos idénticos o similares. Las tarifas se calcularán conforme a los principios contables aplicables a los sujetos correspondientes y de acuerdo con la normativa aplicable.

6. Se podrán aplicar tarifas diferenciadas según se trate de reutilización con fines comerciales o no comerciales.

7. Los sujetos previstos en el artículo 2 publicarán por medios electrónicos, siempre que sea posible y apropiado, las tarifas fijadas para la reutilización de documentos que estén en su poder, así como las condiciones aplicables y el importe real de los mismos, incluida la base de cálculo utilizada.

En el resto de los casos en que se aplique una tarifa, el sujeto de que se trate indicará por adelantado qué factores se tendrán en cuenta para el cálculo de la misma. Cuando se solicite, dicho sujeto también indicará cómo se ha calculado esa tarifa en relación con la solicitud de reutilización concreta.

8. Cuando las tarifas a exigir tengan la naturaleza de tasa, su establecimiento y la regulación de sus elementos esenciales se ajustarán a lo previsto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, y demás normativa tributaria.

9. En todo caso, los usuarios podrán reutilizar gratuitamente:

a) Los conjuntos de datos de alto valor mencionados en el artículo 3 ter salvo que:

1.º) Se trate de documentos de bibliotecas, incluidas las universitarias, los museos y los archivos.

2.º) Se trate de documentos en poder de sociedades mercantiles públicas previstas en el párrafo c) del artículo 2, cuando el hecho de poner a disposición dichos conjuntos de datos de manera gratuita pudiera provocar una distorsión de la competencia en los mercados correspondientes.

3.º) Cuando el hecho de poner a disposición de forma gratuita conjuntos de datos de alto valor pueda tener un impacto sustancial en el presupuesto de organismos o entidades de derecho público que deban obtener ingresos para financiar su actividad de servicio público, en cuyo caso la Administración Pública a la que estén vinculados o de la que dependan podrá eximir a tales organismos o entidades de la obligación de poner a disposición de forma gratuita los conjuntos de datos de alto valor, por un período no superior a los dos años a partir de la entrada en vigor del acto de ejecución o resolución que apruebe la lista de conjuntos de datos de alto valor.

b) Los datos de investigación previstos en el artículo 1 de esta ley.

Artículo 8. *Condiciones de reutilización.*

La reutilización de la información de los sujetos previstos en el artículo 2 podrá estar sometida, entre otras, a las siguientes condiciones generales:

a) Que el contenido de la información, incluyendo sus metadatos, no sea alterado.
b) Que no se desnaturalice el sentido de la información.
c) Que se cite la fuente.
d) Que se mencione la fecha de la última actualización.

e) Cuando la información contenga datos de carácter personal, la finalidad o finalidades concretas para las que es posible la reutilización futura de los datos.

f) Cuando la información, aún siendo facilitada de forma disociada, contuviera elementos suficientes que pudieran permitir la identificación de los interesados en el proceso de reutilización, la prohibición de revertir el procedimiento de disociación mediante la adición de nuevos datos obtenidos de otras fuentes.

Artículo 9. *Licencias.*

1. Las Administraciones y organismos del sector público incluidos dentro del ámbito de aplicación de esta Ley, fomentarán el uso de licencias abiertas con las mínimas restricciones posibles sobre la reutilización de la información.

2. En los casos en los que se otorgue una licencia, ésta deberá reflejar, al menos, la información relativa a la finalidad concreta para la que se concede la reutilización, indicando igualmente si la misma podrá ser comercial o no comercial, para la que se concede la reutilización, la duración de la licencia, las obligaciones del beneficiario y del organismo concedente, las responsabilidades de uso y modalidades financieras, indicándose el carácter gratuito o, en su caso, la tarifa aplicable.

TÍTULO III

Procedimiento y régimen sancionador

Artículo 10. *Procedimiento de tramitación de solicitudes de reutilización.*

1. Las solicitudes de reutilización de documentos administrativos deberán dirigirse al órgano competente, entendiendo por tal aquel en cuyo poder obren los documentos cuya reutilización se solicita. Las solicitudes se presentarán por aquellas personas físicas o jurídicas que pretendan reutilizar los documentos de conformidad con lo previsto en esta Ley.

No obstante, cuando el órgano al que se ha dirigido la solicitud no posea la información requerida pero tenga conocimiento del sujeto previsto en el artículo 2 que la posee, le remitirá a la mayor brevedad posible la solicitud dando cuenta de ello al solicitante.

Cuando ello no sea posible, informará directamente al solicitante sobre el sujeto previsto en el artículo 2 al que, según su conocimiento, ha de dirigirse para solicitar dicha información.

2. La solicitud deberá reflejar el contenido previsto en el artículo 66.1 de la Ley 39/2015, de 1 de octubre, identificando el documento o documentos susceptibles de reutilización y especificando los fines, comerciales o no comerciales, de la reutilización. No obstante, cuando una solicitud esté formulada de manera imprecisa, el órgano competente pedirá al solicitante que la concrete y le indicará expresamente que si así no lo hiciera se le tendrá por desistido de su solicitud, en los términos previstos en el artículo 68 de la Ley 39/2015, de 1 de octubre. El solicitante deberá concretar su petición en el plazo de diez días a contar desde el día siguiente al de la recepción de dicho requerimiento. A estos efectos, el órgano competente asistirá al solicitante para delimitar el contenido de la información solicitada.

El cómputo del plazo para resolver la solicitud de información se entenderá suspendido por el tiempo que medie entre la notificación del requerimiento y su efectivo cumplimiento por el destinatario o, en su defecto, por el transcurso del plazo concedido, informándose al solicitante de la suspensión del plazo para resolver.

3. El órgano competente resolverá las solicitudes de reutilización en el plazo máximo de veinte días desde la recepción de la solicitud en el registro del órgano competente para su tramitación, con carácter general. Cuando por el volumen y la complejidad de la información solicitada resulte imposible cumplir el citado plazo se podrá ampliar el plazo de resolución en otros veinte días. En este caso deberá informarse al solicitante, en el plazo máximo de diez días, de toda ampliación del plazo, así como de las razones que lo justifican.

4. Las resoluciones que tengan carácter estimatorio podrán autorizar la reutilización de los documentos sin condiciones o bien supondrán el otorgamiento de la oportuna licencia para su reutilización en las condiciones pertinentes impuestas a través de la misma. En todo

caso la resolución estimatoria supondrá la puesta a disposición del documento en el mismo plazo previsto en el apartado anterior para resolver.

5. Si la resolución denegara total o parcialmente la reutilización solicitada, se notificará al solicitante, comunicándole los motivos de dicha negativa en los plazos mencionados en el apartado 3, motivos que habrán de estar fundados en alguna de las disposiciones de esta Ley o en el ordenamiento jurídico vigente.

6. En caso de que la resolución desestimatoria esté fundada en la existencia de derechos de propiedad intelectual o industrial por parte de terceros, el órgano competente deberá incluir una referencia a la persona física o jurídica titular de los derechos cuando ésta sea conocida, o, alternativamente, al cedente del que el organismo haya obtenido los documentos. Las bibliotecas, incluidas las universitarias, los museos y los archivos no estarán obligadas a incluir tal referencia.

7. En todo caso, las resoluciones adoptadas deberán contener una referencia a las vías de recurso a que pueda acogerse en su caso el solicitante, en los términos previstos en el artículo 40 de la Ley 39/2015, de 1 de octubre.

8. Si en el plazo máximo previsto para resolver y notificar no se hubiese dictado resolución expresa, el solicitante podrá entender desestimada su solicitud.

9. Las sociedades mercantiles públicas previstas en el párrafo c) del artículo 2, los centros de enseñanza, las organizaciones que realicen actividades de investigación o que financien tales actividades no estarán obligadas a cumplir lo previsto en este artículo.

Artículo 10.bis. *Unidad responsable de información.*

1. Cada sujeto previsto en el artículo 2 determinará la Unidad responsable de garantizar la puesta a disposición de su información.

2. En la Administración General del Estado se designarán las Unidades responsables de información en el ámbito de las Subsecretarías de cada Departamento. Los restantes sujetos previstos en el artículo 2 del sector público estatal con personalidad jurídica propia designarán sus Unidades correspondientes.

3. La Unidad responsable de información tendrá las siguientes funciones:

a) Coordinar las actividades de reutilización de la información con las políticas existentes en materia de publicaciones, información administrativa y administración electrónica.

b) Facilitar información sobre los órganos competentes, dentro de su ámbito, para la recepción, tramitación y resolución de las solicitudes de reutilización que se tramiten de acuerdo con lo previsto en el artículo 10.

c) Promover que la información sea provista en los formatos adecuados y esté actualizada en la medida de lo posible.

d) Coordinar y fomentar las actividades de promoción, concienciación y formación.

Artículo 11. *Régimen sancionador.*

1. En el ámbito de la Administración General del Estado, se considerarán infracciones muy graves a lo previsto en esta ley:

a) La desnaturalización del sentido de la información para cuya reutilización se haya concedido una licencia;

b) La alteración muy grave del contenido de la información para cuya reutilización se haya concedido una licencia.

2. Se considerarán infracciones graves:

a) La reutilización de documentación sin haber obtenido la correspondiente licencia en los casos en que ésta sea requerida;

b) La reutilización de la información para una finalidad distinta a la que se concedió;

c) La alteración grave del contenido de la información para cuya reutilización se haya concedido una licencia;

d) El incumplimiento grave de otras condiciones impuestas en la correspondiente licencia o en la normativa reguladora aplicable.

3. Se considerarán infracciones leves:

a) La falta de mención de la fecha de la última actualización de la información;
b) La alteración leve del contenido de la información para cuya reutilización se haya concedido una licencia;
c) La ausencia de cita de la fuente de acuerdo con lo previsto en el artículo 8 de esta ley;
d) El incumplimiento leve de otras condiciones impuestas en la correspondiente licencia o en la normativa reguladora aplicable.

4. Por la comisión de las infracciones recogidas en este artículo, se impondrán las siguientes sanciones:

a) Sanción de multa de 50.001 a 100.000 euros por la comisión de infracciones muy graves;
b) Sanción de multa de 10.001 a 50.000 euros por la comisión de infracciones graves;
c) Sanción de multa de 1.000 a 10.000 euros. Por la comisión de infracciones leves.

Por la comisión de infracciones muy graves y graves recogidas, además de las sanciones previstas en las letras a) y b), se podrá sancionar con la prohibición de reutilizar documentos sometidos a licencia durante un periodo de tiempo entre 1 y 5 años y con la revocación de la licencia concedida.
5. Las sanciones se graduarán atendiendo a la naturaleza de la información reutilizada, al volumen de dicha información, a los beneficios obtenidos, al grado de intencionalidad, a los daños y perjuicios causados, en particular a los que se refieren a la protección de datos de carácter personal, a la reincidencia y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.
6. La potestad sancionadora se ejercerá, en todo lo no previsto en la presente ley, de conformidad con lo dispuesto en el Capítulo III de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. Su ejercicio corresponderá a los órganos competentes que la tengan atribuida por razón de la materia.
7. El régimen sancionador previsto en esta ley se entiende sin perjuicio de la responsabilidad civil o penal en que pudiera incurrirse, que se hará efectiva de acuerdo con las correspondientes normas legales.

Disposición adicional primera. *Planes y programas.*

El Gobierno, a propuesta de los Ministerios competentes, desarrollará planes y programas de actuaciones dirigidos a facilitar la reutilización de la información del sector público en aras de promover el crecimiento del sector de contenidos digitales, pudiendo establecer con el resto de las Administraciones públicas los mecanismos de colaboración que se estimen pertinentes para la consecución de dicho objetivo.

Disposición adicional segunda. *Aplicación a otros organismos.*

1. Lo previsto en esta ley será de aplicación a los documentos conservados por organismos e instituciones diferentes a los mencionados en el artículo 2, a los que, en los términos previstos en su normativa reguladora, resulte aplicable en su actividad la Ley 39/2015, de 1 de octubre.
2. Las previsiones contenidas en la presente ley serán de aplicación a las sentencias y resoluciones judiciales, sin perjuicio de lo previsto en el artículo 107.10 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y su desarrollo específico.

Disposición adicional tercera. *Transferencia para Reutilización Pública de Microdatos de Encuestas correspondientes a Investigaciones Sociológicas.*

1. Los proyectos de investigación, análisis, o diagnóstico social que vayan a ser desarrollados por los sujetos relacionados en el artículo 2.a), b), c) y d) siempre que impliquen la realización de encuestas cuantitativas en el ámbito de las ciencias sociales con toma de datos, deberán incorporar en su diseño un plan para la inclusión de la documentación y microdatos anonimizados de dicha encuesta en un Banco de Datos específico, creado en el Centro de Investigaciones Sociológicas. Este Plan se depositará en el mencionado Banco de Datos en los 12 meses posteriores a la aprobación del proyecto, y

los microdatos anonimizados que integren el estudio deberán transferirse en un periodo no superior a cuatro años desde la aprobación del proyecto. Este plazo podrá ser ampliado excepcionalmente por causas derivadas del desarrollo y conclusión del proyecto.

2. No obstante lo dispuesto en el apartado anterior, quedan excluidas de tal obligación:

a) Las encuestas realizadas por Agencias Estatales, las entidades públicas empresariales, las sociedades mercantiles estatales, las fundaciones públicas y las entidades de Derecho Público con independencia funcional o con una especial autonomía reconocida por la Ley cuando actúen en régimen de derecho privado.

b) Las realizadas por la Sociedad Estatal de Participaciones Industriales, o cualquiera de las empresas o fundaciones de su Grupo, el Instituto Nacional de Estadística (INE) y los organismos similares de las Comunidades Autónomas.

c) Las encuestas que conformen las estadísticas de carácter oficial incluidas en los correspondientes Planes Estadísticos Nacionales y sujetas a la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, así como las estadísticas europeas sujetas a su normativa específica. No obstante, en este caso, el INE impulsará, como coordinador del Sistema Estadístico de la Administración del Estado, que se dé la publicidad debida a los microdatos de estas encuestas con finalidad estadística elaboradas por estos organismos.

3. No serán objeto de transferencia los microdatos obtenidos de registros administrativos de datos, así como los utilizados para las encuestas que sean determinantes o indispensables para la política estratégica interna de las entidades que las lleven a cabo en los términos que se determine reglamentariamente.

4. Las empresas, equipos de investigación particulares y personas físicas o jurídicas que realicen asimismo este tipo de proyectos a través encuestas cuantitativas en el ámbito de las ciencias sociales con toma de datos, y que reciban ayudas o subvenciones públicas, siempre que las mismas supongan más del 50% de los fondos con que se financien sus proyectos de investigación, estarán igualmente sometidas a la presentación del plan y a la obligación de transferir los datos para la obtención de la misma. En la normativa reguladora del régimen subvencional de ayudas públicas para este tipo de proyectos y en sus sucesivas convocatorias, especialmente aquellas derivadas del Plan Nacional de I+D+i y el Plan Nacional de la Ciencia, se harán constar estas obligaciones. No obstante, respecto de estos sujetos será aplicable la misma posibilidad de exclusión cuando la publicación de los microdatos pudiera causar un perjuicio competitivo irreparable en su posicionamiento empresarial en el mercado.

5. El incumplimiento de esta obligación por parte de los equipos investigadores responsables, especialmente en el marco de los Planes Nacionales de Investigación Científica, Desarrollo e Innovación Tecnológica, supondrá causa de exclusión a la hora de solicitar nuevas ayudas de financiación pública, de acuerdo con los procedimientos sancionadores previstos en la Ley 38/2003, de 17 de noviembre, General de Subvenciones.

Disposición adicional cuarta. *Reutilización de documentos, archivos y colecciones de origen privado.*

En cuanto a los documentos, archivos y colecciones de origen privado, conservadas en los archivos, bibliotecas (incluidas las universitarias) y museos, su puesta a disposición con fines de reutilización, ha de respetar las condiciones establecidas en el instrumento jurídico correspondiente que haya dado lugar a la conservación y custodia de estos fondos en instituciones culturales públicas.

Disposición adicional quinta. *Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos).*

Con relación a la reutilización de determinadas categorías de datos protegidos a que se refiere el capítulo II del Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos) que obren en poder de los sujetos previstos en los párrafos a) y b) de esta ley, sin perjuicio de la aplicación

directa de los preceptos de dicho Reglamento, se aplicarán asimismo las siguientes previsiones:

a) El régimen sancionador previsto en el artículo 11 de esta ley, en el ámbito de la Administración General del Estado, y a tal efecto:

1.º Se considerará infracción muy grave de las previstas en el artículo 11.1 el incumplimiento de las condiciones de acceso a los datos protegidos o de las condiciones impuestas para preservar la seguridad e integridad del entorno de tratamiento seguro utilizado.

2.º Se considerarán infracciones graves de las previstas en el artículo 11.2, las siguientes:

i. El incumplimiento por el reutilizador de su compromiso formal de confidencialidad que prohíba la divulgación de la información contenida en las categorías de datos protegidos.

ii. La reidentificación por el reutilizador de los interesados a quienes se refieran los datos protegidos.

iii. La falta de notificación de los incidentes de seguridad o cualquier otra violación de la seguridad de los datos protegidos reutilizados que den lugar o conlleven riesgo de reidentificación de los interesados.

b) Los sujetos previstos en los párrafos a) y b) del artículo 2 que permitan la reutilización de las categorías de datos protegidos podrán exigir el pago de una tasa por la misma, que se calculará en función de los costes relacionados con la tramitación de las solicitudes de reutilización de las categorías de datos enumeradas en el artículo 3.1 del Reglamento y se limitará a los costes necesarios en relación con:

i. La reproducción, la entrega y la difusión de los datos;

ii. La adquisición de derechos;

iii. La anonimización u otras formas de preparación de los datos personales y de los datos comerciales confidenciales con arreglo a lo dispuesto en el artículo 5.3 del Reglamento;

iv. El mantenimiento del entorno de tratamiento seguro;

v. La adquisición, por parte de terceros ajenos al sector público, del derecho de terceros de permitir la reutilización de conformidad con el capítulo II del Reglamento, y

vi. La asistencia a los reutilizadores en la obtención del consentimiento de los interesados y del permiso de los titulares de datos cuyos derechos e intereses puedan verse afectados por la reutilización.

El establecimiento y la regulación de los elementos esenciales de dicha tasa deberá ajustarse a lo previsto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos y demás normativa tributaria aplicable. En todo caso deberá ser transparente, no discriminatoria y proporcionada, estar justificada objetivamente y respetar las restantes condiciones contempladas en el artículo 6 del Reglamento.

c) Con relación al procedimiento de tramitación de solicitudes de datos protegidos se aplicará lo dispuesto en el artículo 5 del Reglamento y el artículo 10 de la ley, con las siguientes especialidades:

i. El plazo para resolver el procedimiento será de dos meses a contar desde la recepción de la solicitud por el órgano competente.

ii. Cuando la solicitud sea excepcionalmente extensa o compleja, el órgano competente para dictar resolución podrá ampliar el plazo para resolver hasta un máximo de 30 días previa notificación al interesado en los términos previstos en el artículo 32 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las administraciones públicas.

Contra la resolución que se dicte concediendo o denegando la reutilización, el interesado podrá interponer los recursos que procedan en vía administrativa y jurisdiccional, de conformidad con lo establecido en la Ley 39/2015, de 1 de octubre, y en la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Si en el plazo máximo previsto para resolver y notificar no se hubiese dictado resolución expresa, el solicitante podrá entender desestimada su solicitud.

Los sujetos previstos en los párrafos a) y b) del artículo 2 comunicarán al Ministerio de Asuntos Económicos y Transformación Digital la identidad de los organismos competentes para prestar asistencia designados, en su caso, en virtud del artículo 5.1 del Reglamento, con objeto de dar cumplimiento a las previsiones de notificación a la Comisión previstas en el artículo 7.5 del mismo. Asimismo, comunicarán toda modificación posterior de la identidad de dichos organismos competentes.

Disposición transitoria única. *Régimen transitorio aplicable a los acuerdos exclusivos.*

Los acuerdos exclusivos existentes a 17 de julio de 2013 a los que no se aplique la excepción contemplada en los apartados 2 y 3 del artículo 6 y que fuesen celebrados por los sujetos previstos en los párrafos a) y b) del artículo 2 concluirán cuando expire el contrato o, en cualquier caso, no más tarde del 18 de julio de 2043.

Sin perjuicio de lo previsto en el párrafo anterior, los acuerdos exclusivos existentes a 16 de julio de 2019 a los que no se apliquen las excepciones contempladas en los apartados 2 y 3 del artículo 6 que fuesen celebrados por los sujetos previstos en el párrafo c) del artículo 2, concluirán cuando expire el contrato o, en cualquier caso, no más tarde del 17 de julio de 2049.

Disposición final primera. *Fundamento constitucional.*

La presente ley tiene carácter de legislación básica al amparo de lo dispuesto en el artículo 149.1.18 ª de la Constitución Española. Se exceptúan los apartados 1 (párrafos segundo y tercero), 3 y 8 del artículo 10, el apartado 2 del artículo 10.bis. y el artículo 11.

Disposición final segunda. *Desarrollo reglamentario.*

El Gobierno, en el ámbito de sus competencias, dictará cuantas disposiciones sean necesarias para la ejecución y desarrollo de lo establecido en esta ley.

Disposición final tercera. *Entrada en vigor.*

Esta Ley entrará en vigor a los dos meses de su publicación en el «Boletín Oficial del Estado».

Anexo

Definiciones

A efectos de la presente Ley, se entiende por:

1) Anonimización: Proceso por el que se transforman documentos en documentos anónimos que no se refiere a una persona física identificada o identificable o al proceso de convertir datos personales que se hayan anonimizado, de forma que el interesado no sea identificable o haya dejado de serlo.

2) Conjuntos de datos de alto valor: Documentos cuya reutilización está asociada a considerables beneficios para la sociedad, el medio ambiente y la economía, en particular debido a su idoneidad para la creación de servicios de valor añadido, aplicaciones y puestos de trabajo nuevos, dignos y de calidad, y del número de beneficiarios potenciales de los servicios de valor añadido y aplicaciones basados en tales conjuntos de datos.

3) Datos abiertos: Son aquellos que cualquiera es libre de utilizar, reutilizar y redistribuir, con el único límite, en su caso, del requisito de atribución de su fuente o reconocimiento de su autoría.

4) Datos dinámicos: Documentos en formato digital, sujetos a actualizaciones frecuentes o en tiempo real, debido, en particular, a su volatilidad o rápida obsolescencia; los datos generados por los sensores suelen considerarse datos dinámicos.

5) Datos de investigación: Documentos en formato digital, distintos de las publicaciones científicas, recopilados o elaborados en el transcurso de actividades de investigación científica y utilizados como prueba en el proceso de investigación, o comúnmente aceptados

en la comunidad investigadora como necesarios para validar las conclusiones y los resultados de la investigación.

6) Documento: Toda información o parte de ella, cualquiera que sea su soporte o forma de expresión, sea esta textual, gráfica, sonora visual o audiovisual, incluyendo los metadatos asociados y los datos contenidos con los niveles más elevados de precisión y desagregación. A estos efectos no se considerarán documentos los programas informáticos que estén protegidos por la legislación específica aplicable a los mismos.

7) Formato legible por máquina: Un formato de archivo estructurado que permita a las aplicaciones informáticas identificar, reconocer y extraer con facilidad datos específicos, incluidas las declaraciones fácticas y su estructura interna.

8) Formato abierto: Un formato de archivo independiente de plataformas y puesto a disposición del público sin restricciones que impidan la reutilización de los documentos.

9) Licencia tipo: Conjunto de condiciones de reutilización predefinidas en formato digital, preferiblemente compatibles con licencias modelo públicas disponibles en línea.

10) Norma formal abierta: Una norma establecida por escrito que especifica los criterios de interoperabilidad de la aplicación informática.

11) Tercero: Toda persona física o jurídica distinta de un sujeto previsto en el artículo 2 que esté en posesión de los datos.

12) Universidad: Todo organismo del sector público que imparta enseñanza superior post-secundaria conducente a la obtención de títulos académicos.

§ 56

Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal

Ministerio de la Presidencia
«BOE» núm. 269, de 8 de noviembre de 2011
Última modificación: sin modificaciones
Referencia: BOE-A-2011-17560

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, por medio de la cual se incorpora a nuestro ordenamiento jurídico la Directiva 2003/98/CE, de 17 de noviembre de 2003, del Parlamento Europeo y del Consejo, relativa a la reutilización de la información del sector público, establece el régimen jurídico general para la reutilización de dicha información.

La citada ley reconoce la importancia y el valor que tiene la información generada desde las instancias públicas por el interés que posee para las empresas y, consecuentemente, para el crecimiento económico y la creación de empleo. Asimismo, señala el interés de la citada información para los ciudadanos y ciudadanas, como elemento de apertura y participación democrática.

La Ley 37/2007, de 16 de noviembre, no modifica el régimen de acceso a los documentos administrativos consagrado en nuestro ordenamiento jurídico, sino que aporta un valor añadido al derecho de acceso, contemplando el régimen normativo básico para el uso por parte de terceros de la información que obra en poder del sector público, con fines comerciales o no comerciales, en un marco de libre competencia, regulando las condiciones mínimas a las que debe acogerse un segundo nivel de tratamiento de la información. En este sentido, la Ley 37/2007, de 16 de noviembre, establece las bases para promover la reutilización de la información pública y garantiza que ésta se lleve a cabo en el marco de unas condiciones claras, transparentes y no discriminatorias.

Por otra parte, favorecer la reutilización de la información pública figura entre los objetivos políticos establecidos para la Administración Electrónica en la Declaración Ministerial de Malmö, de noviembre de 2009, que fija las prioridades de la Unión Europea dentro de este ámbito para el periodo 2010-2015, y han sido desarrolladas en el Plan de Acción de la Unión Europea sobre Administración Electrónica en el período 2011-2015. Este objetivo se ha visto consolidado en la Declaración Ministerial de Granada, de abril de 2010, y en la nueva Agenda Digital Europea, de mayo de 2010, que guiará el futuro de la Unión Europea en materia de sociedad de la información hasta el año 2015.

El presente real decreto se enmarca en el conjunto de medidas que constituyen la Estrategia 2011-2015 del Plan Avanza 2, que prevé entre sus medidas normativas el desarrollo reglamentario de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, al objeto de detallar para el ámbito del sector público estatal

las disposiciones de esta Ley, promoviendo y facilitando al máximo la puesta a disposición de la información del sector público.

El capítulo I del real decreto establece en el artículo 1 su objeto y ámbito de aplicación, manteniendo el ámbito de aplicación objetiva de la Ley 37/2007, de 16 de noviembre, y acotando su ámbito de aplicación subjetiva al sector público estatal.

El capítulo II del real decreto contiene el régimen jurídico de la reutilización de la información del sector público estatal. Así, el artículo 2 establece el principio general de que, en el ámbito del sector público estatal, estará autorizada la reutilización de los documentos elaborados o custodiados por las personas jurídico-públicas que lo forman, sin perjuicio del régimen aplicable al derecho de acceso a los documentos establecido en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y de las demás normas que regulan el derecho de acceso o la publicidad registral con carácter específico.

El artículo 3 del real decreto tiene por objeto regular determinadas responsabilidades y funciones en materia de reutilización en cada departamento ministerial, organismo o entidad del sector público.

El artículo 4 del real decreto supone un desarrollo de lo dispuesto en el apartado 5 del artículo 4 de la Ley 37/2007, de 16 de noviembre. En este artículo se establece que las entidades del sector público estatal informarán, a través de su sede electrónica, sobre los documentos reutilizables elaborados o custodiados por ellas. La publicación de la información sobre los documentos reutilizables en la sede electrónica, prevista en el artículo 4 no implica necesariamente que los propios documentos reutilizables se pongan a disposición del público a través de la sede electrónica, siendo posible que dicha puesta a disposición se realice a través de páginas de Internet u otros medios electrónicos.

El artículo 5 prevé el mantenimiento de un catálogo de información pública reutilizable correspondiente, al menos, a la Administración General del Estado y demás organismos y entidades que forman parte del sector público estatal, que permitirá acceder desde un único punto a los recursos de información pública reutilizable existentes.

El artículo 6 establece determinados mecanismos de coordinación pertinentes en el ámbito del sector público estatal, en particular, en lo que se refiere a la puesta a disposición de información reutilizable por medios electrónicos.

El capítulo III desarrolla el régimen de modalidades de reutilización de los documentos reutilizables establecido en la Ley 37/2007, de 16 de noviembre, promoviendo al máximo la homogeneidad, claridad y sencillez del régimen de condiciones aplicables a la reutilización, contribuyendo de este modo al mayor aprovechamiento de las posibilidades de reutilización y a impulsar la competencia y la innovación.

El artículo 7 establece ciertas condiciones generales para la reutilización de la información, exigibles en todo caso, que constituyen un desarrollo de los contenidos potestativos establecidos en el artículo 8 de la Ley 37/2007, de 16 de noviembre. Entre otras condiciones, se prohíbe que el sentido de la información sea desnaturalizado, es decir, que sea tergiversado o falseado.

El apartado 1 del artículo 8 establece que, en el ámbito subjetivo de aplicación del real decreto, la modalidad general de puesta a disposición de los documentos reutilizables será la puesta a disposición para la reutilización sin sujeción a condiciones específicas, siendo únicamente aplicables las condiciones generales antes mencionadas. De este modo, el real decreto establece como regla general de aplicación la modalidad más favorable a la reutilización, que deberá ser la que se siga en la generalidad de los casos. No obstante, para los supuestos en los que la modalidad general de puesta a disposición no resulte adecuada, se puede considerar el establecimiento de condiciones específicas adicionales a las condiciones generales previstas en este artículo. En tales supuestos, se podrá optar por aplicar alguna de las otras modalidades de puesta a disposición establecidas en la Ley 37/2007, de 16 de noviembre, en los términos desarrollados por los apartados 2 a 4 del artículo 8 del real decreto. Asimismo, se prevé que la puesta a disposición a través del procedimiento de solicitud previa establecido en el artículo 10 de la Ley 37/2007, de 16 de noviembre, sólo sea empleado cuando la naturaleza de los documentos así lo exija, por ejemplo, cuando correspondan a documentos que no preexistan en formato electrónico y en otros casos excepcionales debidamente motivados.

El capítulo IV regula el régimen aplicable a los documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales.

Conforme a lo establecido en el artículo 3.3 de la Ley 37/2007, de 16 de noviembre, el artículo 9 prevé que la reutilización de los documentos sobre los que existan derechos de propiedad intelectual o industrial de terceros sólo podrá ser autorizada si se dispone de la preceptiva y suficiente cesión de los derechos de explotación por parte de las personas titulares de los mismos.

Por su parte, el artículo 10 desarrolla el mandato establecido en el artículo 3.3.e), de la Ley 37/2007, de 16 de noviembre, de que el ejercicio de los derechos de propiedad intelectual de las Administraciones y organismos del sector público sobre sus documentos deberá realizarse de forma que se facilite su reutilización, previendo que la puesta a disposición de los documentos para su reutilización conllevará la cesión no exclusiva de los derechos de propiedad intelectual correspondientes.

Finalmente, el artículo 11 establece, en relación con los documentos que contengan datos de carácter personal, que podrá procederse a autorizar su reutilización siempre y cuando se proceda previamente a un proceso de disociación, de conformidad con lo establecido en la normativa de protección de datos de carácter personal.

Conforme a lo dispuesto por el artículo 14.11 de la Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres, el uso del masculino genérico en el texto de esta disposición debe considerarse como inclusivo de ambos géneros.

El presente real decreto se dicta en virtud de la habilitación contenida en la disposición final segunda de la Ley 37/2007, de 16 de noviembre y ha sido informado por el Consejo Superior de Administración Electrónica y el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información y sometido a consulta pública.

En su virtud, a propuesta del Ministro de Industria, Turismo y Comercio, y del Vicepresidente del Gobierno de Política Territorial y Ministro de Política Territorial y Administración Pública, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de octubre de 2011,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente real decreto tiene por objeto desarrollar la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, en el ámbito del sector público estatal, en lo relativo al régimen jurídico de la reutilización, las obligaciones del sector público estatal, las modalidades de reutilización de los documentos reutilizables y el régimen aplicable a documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales.

2. Se entiende que forman parte del sector público estatal, a los efectos de esta norma, los siguientes entes, organismos y entidades:

a) La Administración General del Estado.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social.

c) Los organismos autónomos y las agencias estatales dependientes de la Administración General del Estado.

d) Las entidades de derecho público dependientes de la Administración General del Estado o vinculadas a ella, que cumplan los requisitos del artículo 2.d) de la Ley 37/2007, de 16 de noviembre.

e) Las entidades estatales de derecho público distintas a las mencionadas en los párrafos c) y d) de este apartado y que, con independencia funcional o con una especial autonomía reconocida por ley, tengan atribuidas funciones de regulación o control de carácter externo sobre un determinado sector o actividad.

f) Las fundaciones del sector público estatal, definidas en el artículo 44 de la Ley 50/2002, de 26 de diciembre, de Fundaciones.

g) Los consorcios, formados por entes, entidades u organismos del sector público estatal, dotados de personalidad jurídica propia.

h) Las asociaciones constituidas por las Administraciones, organismos y entidades mencionados en los párrafos anteriores de este apartado.

3. El presente real decreto se aplicará a los documentos elaborados o custodiados por el sector público estatal cuya reutilización esté autorizada conforme a la Ley 37/2007, de 16 de noviembre y a esta norma y que no se encuentren recogidos en las excepciones previstas en el artículo 3 de la misma Ley.

4. Lo previsto en este real decreto no restringirá las previsiones más favorables que, sobre acceso o reutilización de la información, se establezcan en las disposiciones sectoriales específicas.

5. A los efectos de esta norma se entiende por «agente reutilizador» toda persona, física o jurídica que reutilice información del sector público, ya sea para fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública.

CAPÍTULO II

Régimen jurídico y organizativo de la reutilización de la información en el sector público estatal

Artículo 2. *Autorización general para la reutilización de los documentos del sector público y puesta a disposición por medios electrónicos.*

1. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 autorizarán la reutilización de los documentos elaborados o custodiados por ellos e incluidos en el ámbito de aplicación de este real decreto, sin perjuicio de lo dispuesto en el régimen aplicable al derecho de acceso a los documentos en virtud de lo previsto en el artículo 37 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y las demás normas que regulan el derecho de acceso, la reutilización de la información del sector público o la publicidad registral con carácter específico. Únicamente podrá denegarse motivadamente la reutilización de los documentos si concurre alguno de los supuestos establecidos en el apartado 3 del artículo 3 de la Ley 37/2007, de 16 de noviembre.

2. Se pondrán a disposición del público los documentos reutilizables que se encuentren previamente disponibles en formato electrónico por medios electrónicos, de una manera estructurada y usable para los interesados e interesadas y preferentemente en bruto, en formatos procesables y accesibles de modo automatizado correspondientes a estándares abiertos en los términos establecidos en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. Asimismo, los documentos reutilizables y los medios electrónicos de puesta a disposición de los mismos deberán ser accesibles a las personas con discapacidad de acuerdo con la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y su normativa de desarrollo aplicable.

3. Se procurará que la información puesta a disposición se actualice en un tiempo razonable que permita el uso adecuado de dicha información, con una frecuencia análoga con la que actualicen dicha información internamente, así como su disponibilidad, incluida la temporal, completitud e integridad de acuerdo con el marco normativo aplicable en cada caso.

4. Los documentos en formato electrónico reutilizables podrán incluir entre sus metadatos una indicación de su última fecha de actualización y una referencia a las condiciones de reutilización aplicables en cada momento conforme a lo dispuesto en los artículos 7 y 8, en los términos que se establezcan conforme al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

5. Los documentos reutilizables en formato no electrónico serán puestos a disposición del público previa solicitud, en los términos establecidos en el artículo 8.4.

Artículo 3. *Coordinación en materia de reutilización de los órganos, organismos y entidades del sector público estatal.*

1. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 contarán con un órgano encargado de la coordinación de las actividades de reutilización de la información.

En los departamentos ministeriales esta labor de coordinación recaerá en la persona titular de la Subsecretaría del departamento y en los organismos vinculados o dependientes en la persona titular de éstos, sin perjuicio de las atribuciones competenciales que establezcan normas sectoriales específicas y sin perjuicio de las responsabilidades que corresponden a los órganos que deban autorizar la reutilización de la información en cada caso.

En el ejercicio de esa labor de coordinación, corresponderá a dichos órganos:

a) Coordinar las actividades de reutilización de la información con las políticas del departamento u organismo relativas a las publicaciones, la información administrativa y la administración electrónica, así como coordinar la remisión de información sobre las actividades realizadas en materia de reutilización dentro de su ámbito a la Secretaría de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública, que la trasladará al Consejo Superior de Administración Electrónica.

b) Facilitar información sobre los órganos competentes dentro de su ámbito para la recepción, tramitación y resolución de las solicitudes de reutilización que se tramiten de acuerdo con el artículo 10 de la Ley 37/2007, de 16 de noviembre, así como coordinar la provisión de la información sobre los documentos reutilizables prevista en el artículo 4.

c) Resolver, cuando proceda, las quejas y sugerencias que se presenten en materia de reutilización de la información, conforme al Real Decreto 951/2005, de 29 de julio, por el que se establece el marco general para la mejora de la calidad en la Administración General del Estado.

Los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 facilitarán a los correspondientes servicios de información de los Departamentos ministeriales o de dichos organismos y entidades los datos de contacto de aquellos que deban autorizar la reutilización de los documentos elaborados o custodiados por ellos, a efectos de que dichos servicios de información faciliten dichos datos de contacto al público, al menos, por medios electrónicos.

2. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 no serán responsables del uso que de su información hagan los agentes reutilizadores.

3. El ejercicio de la potestad sancionadora, con sujeción a lo establecido en el artículo 11 de la Ley 37/2007, de 16 de noviembre, corresponderá, en el caso de infracciones muy graves, a las personas titulares del departamento ministerial, y en el caso de infracciones graves o leves a los órganos titulares de la información pública correspondiente con rango mínimo de Dirección General. En el caso de los demás organismos mencionados en el artículo 1.2, la competencia corresponderá en todos los casos a la persona titular del organismo, ente o entidad de que se trate.

Artículo 4. *Información sobre los documentos susceptibles de reutilización.*

1. Los órganos de la Administración General del Estado y los demás organismos y entidades a que se hace referencia en el artículo 1.2 informarán de manera estructurada y usable, preferentemente a través de un espacio dedicado de su sede electrónica con la ubicación «sede.gob.es/datosabiertos», sobre qué documentación es susceptible de ser reutilizada, los formatos en que se encuentra disponible, las condiciones aplicables a su reutilización, indicando la fecha de la última actualización de los documentos reutilizables, proporcionando, cuando esté disponible, la información complementaria precisa para su comprensión y procesamiento automatizado y facilitando al máximo la identificación,

búsqueda y recuperación de los documentos disponibles para su reutilización mediante mecanismos tales como listados, bases de datos o índices de información reutilizable.

Igualmente, se informará, preferentemente a través de la correspondiente sede electrónica, sobre la modalidad o, en su caso, modalidades de puesta a disposición de los documentos reutilizables que sean de aplicación conforme a los artículos 7 y 8.

Se procurará que la información sobre los documentos reutilizables prevista en este apartado sea procesable y accesible de modo automatizado.

2. En caso de que apliquen tasas o precios públicos a la reutilización de sus documentos se publicará, preferentemente en la sede electrónica correspondiente, el listado de tasas y precios públicos que sean de aplicación, así como la base de cálculo utilizada para la determinación de los mismos, conforme a lo dispuesto en el artículo 7 de la Ley 37/2007, de 16 de noviembre.

Artículo 5. *Catálogo de Información Pública reutilizable.*

1. La Secretaría de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio mantendrán un catálogo de información pública reutilizable correspondiente, al menos, a la Administración General del Estado y a los demás organismos y entidades a que se refiere el artículo 1.2, que permita acceder, desde un único punto, a los distintos recursos de información pública reutilizable disponibles.

2. Este catálogo será accesible, al menos, desde el punto de acceso general previsto en el artículo 8 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y podrá enlazar e interoperar con iniciativas similares de la propia Administración General del Estado o de otras Administraciones Públicas en las condiciones que se convengan por ambas partes y en el marco de lo previsto en el presente real decreto.

3. Los órganos de la Administración General del Estado y los restantes organismos y entidades enumerados en el artículo 1.2 colaborarán con los departamentos ministeriales mencionados en el apartado 1 para la confección y el mantenimiento de dicho catálogo y asimismo serán responsables de la actualización constante de la información sobre los documentos reutilizables correspondiente a los mismos contenida en el citado catálogo, asegurando la plena coherencia del mismo con la información facilitada conforme al apartado 1 del artículo 4 de este real decreto.

Artículo 6. *Coordinación en materia de reutilización de la información del sector público en el ámbito de la Administración General del Estado.*

1. El Consejo Superior de Administración Electrónica, sin perjuicio de las competencias asignadas a otros órganos, coordinará los aspectos técnicos, necesarios para la aplicación de lo dispuesto en esta norma, relacionados con la reutilización de la información por medios electrónicos.

El Consejo Superior de Administración Electrónica elaborará y publicará durante el tercer trimestre de cada año un informe anual sobre las actividades en materia de reutilización de la información pública por medios electrónicos, tomando en consideración la información que le sea facilitada conforme al párrafo a) del apartado 1 del artículo 3.

2. La Secretaría de Estado para la Función Pública del Ministerio de Política Territorial y Administración Pública y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio ejercerán una función general de promoción de la reutilización de la información del sector público estatal, desarrollando, a tal efecto, actuaciones de información, asesoramiento general y soporte, sensibilización, formación y estudio en materia de reutilización, incluyendo, en su caso, el uso de redes sociales para la construcción de comunidades virtuales de administraciones, ciudadanos y ciudadanas y empresas con interés en la reutilización de la información pública.

3. Sin perjuicio de las competencias atribuidas a otros órganos, el Consejo Superior de Administración Electrónica evaluará periódicamente los aspectos técnicos de los servicios públicos relacionados con la reutilización de la información del sector público, y podrá dirigirse, de oficio o a instancia de parte, a otros órganos de la Administración General del

Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2, para la obtención de información y, en su caso, para la búsqueda de soluciones consensuadas en casos de supuestos de información pública cuya reutilización esté sujeta a restricciones de índole técnica.

CAPÍTULO III

Modalidades de reutilización de los documentos reutilizables

Artículo 7. *Condiciones generales de puesta a disposición de los documentos reutilizables.*

Serán de aplicación las siguientes condiciones generales para todas las modalidades de puesta a disposición de los documentos reutilizables:

a) No desnaturalizar el sentido de la información.

b) Citar la fuente de los documentos objeto de la reutilización.

c) Mencionar la fecha de la última actualización de los documentos objeto de la reutilización, siempre cuando estuviera incluida en el documento original.

d) No se podrá indicar, insinuar o sugerir que los órganos administrativos, organismos o entidades del sector público estatal titulares de la información reutilizada participan, patrocinan o apoyan la reutilización que se lleve a cabo con ella.

e) Conservar y no alterar ni suprimir los metadatos sobre la fecha de actualización y las condiciones de reutilización aplicables incluidos, en su caso, en el documento puesto a disposición para su reutilización por la Administración u organismo del sector público.

Estas condiciones generales serán accesibles mediante un aviso legal por medios electrónicos, de forma permanente, fácil y directa, preferentemente dentro de la ubicación «sede.gob.es/datosabiertos» de la sede electrónica del órgano de la Administración General del Estado, organismo o entidad correspondiente, y vincularán a cualquier agente reutilizador por el mero hecho de hacer uso de los documentos sometidos a ellas.

Dicho aviso legal incluirá el texto contenido en el anexo del presente real decreto.

Artículo 8. *Modalidades de puesta a disposición de los documentos reutilizables.*

1. La modalidad general básica para la puesta a disposición de los documentos reutilizables a que se refiere este real decreto será la puesta a disposición sin sujeción a condiciones específicas, prevista en el párrafo a) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, aplicándose únicamente las condiciones generales establecidas en el artículo 7.

2. No obstante lo dispuesto en el apartado anterior, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2, podrán optar de manera motivada por aplicar las modalidades previstas en los párrafos b) y c) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, a la reutilización de determinados documentos que obren en su poder en los términos que se establecen en los siguientes apartados de este artículo.

A tal efecto, previamente y mediante orden ministerial o resolución del presidente del organismo correspondiente, salvo que por norma legal dicha competencia se atribuya específicamente a un órgano diferente, se determinará el régimen concreto de puesta a disposición aplicable, los documentos reutilizables sometidos al mismo y las condiciones específicas aplicables dentro del marco de lo dispuesto en la Ley 37/2007, de 16 de noviembre y las disposiciones de este real decreto. Las condiciones específicas deberán respetar, en todo caso, los criterios establecidos en el apartado 3 del artículo 4 de la misma Ley y deberán incluir, asimismo, los contenidos mínimos previstos en el artículo 9 de la misma.

3. La modalidad de puesta a disposición conforme al párrafo b) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, se realizará con sujeción a condiciones específicas establecidas en licencias-tipo disponibles en formato digital y procesables electrónicamente. A tal efecto, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 podrán emplear licencias-tipo existentes, denominadas «libres» siempre que se ajusten a lo

establecido en este real decreto y demás normativa aplicable, o proceder a establecer licencias-tipo específicas.

En todo caso, las condiciones específicas establecidas en dichas licencias-tipo para cada tipo de información pública reutilizable serán accesibles por medios electrónicos, de forma permanente, fácil y directa, preferentemente en la sede electrónica del órgano de la Administración General del Estado, organismo o entidad correspondiente de las enumerados en el artículo 1.2, de manera que puedan ser descargadas, almacenadas y reproducidas por los agentes reutilizadores, vinculándoles por el mero hecho de hacer uso de los documentos sometidos a ellas.

Asimismo, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 facilitarán información al público por medios electrónicos sobre las licencias-tipo empleadas por el mismo a lo largo del tiempo y las condiciones específicas aplicables en cada momento, incluyendo expresamente información sobre su período de vigencia y posibles modificaciones de las condiciones específicas aplicables a la reutilización de cada tipo de información pública reutilizable.

Los agentes reutilizadores interesados podrán solicitar a dichos órganos administrativos, organismos y entidades una certificación del contenido de las condiciones específicas aplicables a un tipo de información pública en un momento determinado. Esta certificación será expedida preferentemente mediante medios electrónicos y, en todo caso, en un plazo máximo de 15 días.

4. La modalidad de puesta a disposición previa solicitud conforme al párrafo c) del apartado 2 del artículo 4 de la Ley 37/2007, de 16 de noviembre, se empleará, con carácter general, cuando la naturaleza de los documentos reutilizables exija la tramitación de un procedimiento previa solicitud conforme al artículo 10 de la Ley 37/2007, de 16 de noviembre, por ejemplo, cuando no preexistan en formato electrónico, y en otros casos excepcionales que sean definidos de manera motivada en la correspondiente orden ministerial o resolución del presidente del organismo o entidad correspondiente. Este procedimiento será tramitado preferentemente por medios electrónicos en los términos establecidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y su normativa de desarrollo, figurando el acceso al mismo entre la información sobre la documentación susceptible de ser reutilizada descrita en el artículo 4.

CAPÍTULO IV

Régimen aplicable a documentos reutilizables sujetos a derechos de propiedad intelectual o que contengan datos personales

Artículo 9. *Documentos e información objeto de derechos de propiedad intelectual o industrial de terceros.*

La reutilización de los documentos que custodian los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 sobre los que existan derechos de propiedad intelectual o industrial de terceros sólo podrá ser autorizada si tales órganos, organismos y entidades disponen u obtienen, cuando la reutilización concreta que se vaya a hacer lo exija y en los términos en que sea necesaria, la preceptiva y suficiente cesión de los derechos de explotación por parte de sus titulares.

Artículo 10. *Ejercicio de los derechos de propiedad intelectual de titularidad de los órganos administrativos, organismos o entidades del sector público estatal.*

1. De acuerdo con lo establecido en el artículo 3.3.e) de la Ley 37/2007, de 16 de noviembre, los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 deben ejercer sus derechos de propiedad intelectual sobre sus documentos de forma que se facilite su reutilización.

2. A tal efecto, la puesta a disposición de dichos documentos para su reutilización realizada conforme a lo dispuesto en el artículo 8.1 conllevará la cesión gratuita y no exclusiva de los derechos de propiedad intelectual correspondientes necesarios para

desarrollar la actividad de reutilización autorizada, en cualquier modalidad y bajo cualquier formato, para todo el mundo y por el plazo máximo permitido por la Ley.

No obstante, lo dispuesto en el párrafo anterior podrá ser excepcionado, en todo lo no referente a la no exclusividad de la cesión, mediante el establecimiento de condiciones específicas de acuerdo con lo dispuesto en los apartados 2 a 4 del artículo 8 cuando se empleen las modalidades de puesta a disposición previstas en los mismos, siempre dentro de los límites establecidos en la Ley 37/2007, de 16 de noviembre, y, en particular, en su artículo 4.3 y en su artículo 6.

Artículo 11. *Reutilización de los documentos que contengan datos de carácter personal.*

1. El acceso a documentos que contengan datos de carácter personal o referentes a la intimidad de las personas estará reservado a éstas, que podrán además ejercer sus derechos de rectificación, cancelación y oposición de acuerdo con lo previsto en la legislación de protección de datos personales y el artículo 37.2 de la Ley 30/1992, de 26 de noviembre.

2. No obstante, siempre y cuando los medios técnicos y económicos lo permitan, deberá procederse a la disociación de los datos personales, en los términos que se derivan de lo establecido en el artículo 3.f) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en el artículo 5.1.e) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba su Reglamento de Desarrollo, a fin de permitir su reutilización por otras personas.

Disposición adicional primera. *Ausencia de impacto presupuestario.*

La aplicación de las previsiones contenidas en este real decreto no supondrá incremento del gasto público ni disminución de los ingresos públicos. Por tanto, los departamentos ministeriales, organismos y entidades afectados deben desarrollar las medidas derivadas de su cumplimiento ateniéndose a sus disponibilidades presupuestarias ordinarias, no dando lugar, en ningún caso, a planteamientos de necesidades adicionales de financiación.

Disposición adicional segunda. *Adaptación del sector público estatal a las disposiciones de este real decreto.*

Los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal a que se hace referencia en el artículo 1.2 deberán adaptarse a las disposiciones de este real decreto en el plazo de un año desde su entrada en vigor.

En el citado plazo de un año, aprobarán un plan propio de medidas de impulso de la reutilización de la información del sector público por medios electrónicos, dentro de su ámbito de competencias, que incluirá el compromiso por parte de los departamentos ministeriales de publicar a través de tales medios, de una manera estructurada y usable para los interesados e interesadas y en bruto, en formatos procesables y accesibles de modo automatizado correspondientes a estándares abiertos, al menos cuatro conjuntos de documentos de alto impacto y valor en un plazo máximo de seis meses desde la finalización del plazo de adaptación previsto en el párrafo anterior.

Disposición final primera. *Modificación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.*

El Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, se modifica como sigue:

Uno. Se añade un nuevo párrafo l) al apartado 1 de la disposición adicional primera del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, que tendrá la siguiente redacción:

«l) Reutilización de recursos de información: tratará de las normas comunes sobre la localización, descripción e identificación unívoca de los recursos de

información puestos a disposición del público por medios electrónicos para su reutilización.»

Dos. Se añade una nueva disposición adicional con la siguiente redacción:

«Disposición adicional quinta. *Normativa técnica relativa a la reutilización de recursos de información.*

La normativa relativa a la reutilización de recursos de información deberá estar aprobada a más tardar el 1 de junio de 2012.»

Disposición final segunda. *Habilitación para el desarrollo normativo.*

Por los Ministros de Industria, Turismo y Comercio y de Política Territorial y Administración Pública, se dictarán conjunta o separadamente, según las materias de que se trate, y en el ámbito de sus respectivas competencias, las disposiciones que exijan el desarrollo y aplicación de este real decreto.

Disposición final tercera. *Autorización para la modificación del anexo.*

Se autoriza a que mediante orden del Ministro de la Presidencia, a propuesta conjunta de los Ministros de Industria, Turismo y Comercio, y de Política Territorial y Administración Pública pueda modificarse el contenido del anexo de este real decreto, a fin de mantenerlo actualizado.

Disposición final cuarta. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Aviso legal para la modalidad general de puesta a disposición de los documentos reutilizables regulada en el apartado 1 del artículo 8

1. Conforme a lo dispuesto en el artículo 7 del presente real decreto se incluirá el siguiente texto en el aviso legal disponible por medios electrónicos, preferentemente en la ubicación «sede.gob.es/datosabiertos» de la sede electrónica del órgano administrativo, organismo o entidad correspondiente.

«Obligatoriedad de las condiciones generales.

Las presentes condiciones generales, disponibles con carácter permanente bajo “www.datos.gob.es/avisolegal”, vincularán a cualquier agente reutilizador por el mero hecho de hacer uso de los documentos sometidos a ellas.

Autorización de reutilización y cesión no exclusiva de derechos de propiedad intelectual.

Las presentes condiciones generales permiten la reutilización de los documentos sometidos a ellas para fines comerciales y no comerciales. Se entiende por reutilización el uso de documentos que obran en poder de los órganos de la Administración General del Estado y los demás organismos y entidades del sector público estatal referidos en el artículo 1.2 del Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público estatal, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública. La reutilización autorizada incluye, a modo ilustrativo, actividades como la copia, difusión, modificación, adaptación, extracción, reordenación y combinación de la información.

El concepto de documento es el establecido en el apartado 2 del artículo 3 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, por lo que comprende toda información cualquiera que sea su soporte material o electrónico así como su forma de expresión gráfica, sonora o en imagen utilizada, incluyendo, en consecuencia, también los datos en sus niveles más desagregados o “en bruto”.

Esta autorización conlleva, asimismo, la cesión gratuita y no exclusiva de los derechos de propiedad intelectual, en su caso, correspondientes a tales documentos, autorizándose la realización de actividades de reproducción, distribución, comunicación pública o transformación, necesarias para desarrollar la actividad de reutilización autorizada, en cualquier modalidad y bajo cualquier formato, para todo el mundo y por el plazo máximo permitido por la Ley.

Condiciones generales para la reutilización.

Son de aplicación las siguientes condiciones generales para la reutilización de los documentos sometidos a ellas:

1. Está prohibido desnaturalizar el sentido de la información.
2. Debe citarse la fuente de los documentos objeto de la reutilización. Esta cita podrá realizarse de la siguiente manera: "Origen de los datos: [*órgano administrativo, organismo o entidad del sector público estatal de que se trate*]".
3. Debe mencionarse la fecha de la última actualización de los documentos objeto de la reutilización, siempre cuando estuviera incluida en el documento original.
4. No se podrá indicar, insinuar o sugerir que la [*órgano administrativo, organismo o entidad del sector público estatal de que se trate*] titular de la información reutilizada participa, patrocina o apoya la reutilización que se lleve a cabo con ella.
5. Deben conservarse, no alterarse ni suprimirse los metadatos sobre la fecha de actualización y las condiciones de reutilización aplicables incluidos, en su caso, en el documento puesto a disposición para su reutilización.

Exclusión de responsabilidad.

La utilización de los conjuntos de datos se realizará por parte de los usuarios o agentes de la reutilización bajo su propia cuenta y riesgo, correspondiéndoles en exclusiva a ellos responder frente a terceros por daños que pudieran derivarse de ella.

[El *órgano administrativo, organismo o entidad del sector público estatal de que se trate*] no será responsable del uso que de su información hagan los agentes reutilizadores ni tampoco de los daños sufridos o pérdidas económicas que, de forma directa o indirecta, produzcan o puedan producir perjuicios económicos, materiales o sobre datos, provocados por el uso de la información reutilizada.

[El *órgano administrativo, organismo o entidad del sector público estatal de que se trate*] no garantiza la continuidad en la puesta a disposición de los documentos reutilizables, ni en contenido ni en forma, ni asume responsabilidades por cualquier error u omisión contenido en ellos.

Responsabilidad del agente reutilizador

El agente reutilizador se halla sometido a la normativa aplicable en materia de reutilización de la información del sector público, incluyendo el régimen sancionador previsto en el artículo 11 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.»

2. Con el objetivo de informar a los motores y sistemas automatizados de búsqueda en Internet, se incorporarán además en la codificación de la citada ubicación los mecanismos de localización de información pública reutilizable que se estimen oportunos. Para ello, si bien se podrán utilizar otras modalidades técnicas, se propone el siguiente comando básico, que enlaza con las condiciones generales de reutilización:

Aviso legal

o bien el comando

Aviso legal.

§ 57

Resolución de 21 de marzo de 2013, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Guía de Comunicación Digital para la Administración General del Estado

Ministerio de Hacienda y Administraciones Públicas
«BOE» núm. 79, de 2 de abril de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-3528

En los últimos años, la comunicación con los ciudadanos y las empresas por medios digitales a través de portales web, sedes electrónicas, blogs, o redes sociales, a los que en adelante en esta resolución se denominarán bajo el término genérico de sitios web, ha adquirido una importancia indiscutible para la Administración General del Estado (AGE) conformándose como una herramienta indispensable para la difusión de sus contenidos y para fortalecer la participación ciudadana e impulsar la transparencia de la actividad pública.

Además, cabe recordar que como consecuencia de la aplicación de la Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos y del Título II del Real Decreto 1671/2009, de 6 de noviembre, de desarrollo parcial de dicha Ley, la AGE ofrece actualmente la tramitación electrónica de la práctica totalidad de los servicios administrativos en sus sedes electrónicas.

Los estudios sobre el uso en un futuro próximo de los sitios web de las administraciones públicas coinciden en señalar que su utilización se va a incrementar, en primer lugar, por el perfil de los usuarios, los llamados nativos digitales, cuyo modo de relación natural con las administraciones será a través de los medios digitales y en segundo lugar, por la generalización en el uso de dispositivos móviles de tercera y cuarta generación que permitirán acceder e interactuar con dichos medios digitales con una mayor facilidad.

En este contexto, es esencial reforzar la confianza de los usuarios en los sitios web de la AGE ya sea como medio de información, de participación o para la utilización de los servicios de las sedes electrónicas y es necesario también mejorar la usabilidad y la calidad de dichos sitios web, mediante el impulso de la normalización de características tales como su apariencia y sus condiciones de uso, así como mediante el cumplimiento de los requisitos normativos.

Así, la «Guía de Comunicación Digital para la Administración General del Estado» presenta un marco de criterios, recomendaciones y buenas prácticas a tener en cuenta por los Departamentos y Organismos vinculados o dependientes de la AGE, tanto al crear nuevos sitios web como al dotarlos de contenidos o evolucionar y mantener los sitios ya existentes.

La Guía también recopila la abundante normativa aplicable a los sitios web de la AGE y en particular, en materia de: imagen institucional, multilingüismo, accesibilidad o seguridad.

La presente Guía actualiza: la «Guía para la edición y publicación de las páginas web de la Administración General del Estado» de 2005 y de 2008; el «Borrador de la Guía de

páginas web de la AGE» de 2009 y la «Guía de Sedes electrónicas» de 2010, reuniendo dichos documentos en uno único y ampliándolos con indicaciones a la hora de dotar de contenidos a los sitios web o sobre la presencia de la AGE en las redes sociales, que no se contemplaban en los citados documentos.

La «Guía de Comunicación Digital para la Administración General del Estado» se divide en ocho fascículos, que pueden ser utilizados conjunta o independientemente y dos anexos técnicos.

Los fascículos se refieren a diversas materias como son: Aspectos Generales que trata de la navegación, la legibilidad, las consideraciones técnicas, los sitios para dispositivos móviles y el acceso con autenticación; Imagen Institucional que indica el uso de los logotipos del Gobierno de España en los sitios web, el uso de elementos distintivos de imagen en las redes sociales o la imagen promocional de la administración electrónica; Multilingüismo; Accesibilidad; Seguridad; Aspectos de Comunicación; Tecnologías web 2.0 (blogs, cuentas o perfiles de redes sociales), que contiene las recomendaciones sobre los contenidos y las normas de participación en las redes sociales y por último, Mejora y Mantenimiento en el que se aconseja sobre las técnicas y métricas a utilizar en los sitios web una vez puestos en marcha.

Los anexos técnicos se refieren a los Perfiles, que contiene una descripción de los recursos humanos necesarios para las distintas tareas a realizar en la puesta en marcha o mantenimiento de los sitios web de la AGE y a la Normativa que recopila la legislación ya publicada que es de aplicación en este ámbito.

La «Guía de Comunicación Digital para la Administración General del Estado» ha sido elaborada por el Ministerio de Hacienda y Administraciones Públicas, concretamente por la Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica de la Secretaría de Estado para la Administración Pública, en colaboración con la Secretaría de Estado de Comunicación del Ministerio de la Presidencia.

La presente Guía ha sido informada favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica con la participación de todos los Departamentos Ministeriales a los que les es de aplicación.

Atendiendo a la complejidad y diversidad de aspectos que hay que tener en cuenta al elaborar y mantener los sitios web de la AGE, se considera necesaria la publicación de esta resolución de la Secretaría de Estado de Administraciones Públicas, la cual aprueba e insta a la aplicación de la «Guía de Comunicación Digital para la Administración General del Estado», que aglutina los criterios y recomendaciones y clarifica las instrucciones que deban ser observadas al respecto por los distintos departamentos y organismos de la AGE.

En consecuencia, en virtud de las competencias atribuidas por el artículo 16.1 e), f) y g) del Real Decreto 256/2012, de 27 de enero, por el que se desarrolla la estructura orgánica básica del Ministerio de Hacienda y Administraciones Públicas, resuelvo:

Primero. *Aprobación y aplicación de la «Guía de Comunicación Digital para la Administración General del Estado».*

1. Se aprueba la «Guía de Comunicación Digital para la Administración General del Estado», que estará disponible en el Portal de la Administración Electrónica. (http://www.administracionelectronica.gob.es)

2. Los sitios web, elaborados por los Departamentos u Organismos Públicos vinculados o dependientes de la AGE para cualquier tipo de dispositivo, procurarán observar las recomendaciones, criterios y buenas prácticas establecidos en dicha Guía, de manera gradual en la medida en que sus circunstancias, en cuanto a recursos humanos y disponibilidad presupuestaria, lo permitan.

Segundo. *Actualización de la Guía.*

La Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, oída la Comisión Permanente del Consejo Superior de Administración Electrónica llevará a cabo la actualización de la «Guía de Comunicación Digital para la Administración General del Estado» cuando lo considere necesario.

Tercero. *Difusión de la Guía.*

La presente Guía y sus futuras versiones se distribuirán a los Departamentos y Organismos a través de la Comisión Permanente del Consejo Superior de Administración Electrónica y se publicarán en el apartado de Documentación: Metodologías y Guías del Portal de la Administración Electrónica: http://www.administracionelectronica.gob.es.

Los elementos relativos a la Imagen Institucional para contribuir al cumplimiento de los criterios establecidos en esta Guía se facilitarán a los Departamentos y Organismos en el espacio: http://imagen.funciona.es/ al que se accede a través de la Red SARA.

Cuarto. *Aplicación.*

La «Guía de Comunicación Digital para la Administración General del Estado» que se aprueba mediante la presente Resolución se aplicará desde el día siguiente al de su publicación en el «Boletín Oficial del Estado».

Quinto. *Pérdida de efectos.*

La presente Resolución sustituye a las siguientes disposiciones, que quedan sin efecto:

– «Resolución de 9 de marzo de 2005 de la Secretaria General para la Administración Pública por la que se aprueba la Guía para la edición y publicación de páginas web en la Administración General del Estado».

– El apartado Cuarto y el Anexo II de la "Resolución de 2 de abril de 2007, de la Secretaría General para la Administración Pública (BOE de 16 de abril), por la que se modifica el Manual de Imagen Institucional de la Administración General del Estado y la Guía para la edición y publicación de páginas web en la Administración General del Estado aprobada por Resolución de 9 de marzo de 2005 de la Secretaría General para la Administración Pública."

Información relacionada

- Véase la Resolución de 15 de junio de 2022, por la que se aprueba la actualización del fascículo 2 de la «Guía de Comunicación Digital para la Administración General del Estado», que estará disponible en el Portal de Imagen Institucional https://imagen.funciona.es. Ref. BOE-A-2022-10329
- Véase la Resolución de 21 de septiembre de 2021, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2021-16826
- Véase la Resolución de 28 de febrero de 2020, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2020-3296
- Véase la Resolución de 10 de julio de 2018, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2018-10638
- Véase la Resolución de 3 de abril de 2017, por la que se actualiza el Manual de Imagen Institucional, adaptándolo a la nueva estructura de departamentos ministeriales de la Administración General del Estado. Ref. BOE-A-2017-4178

§ 58

Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial «Boletín Oficial del Estado»

Ministerio de la Presidencia
«BOE» núm. 37, de 12 de febrero de 2008
Última modificación: 24 de septiembre de 2022
Referencia: BOE-A-2008-2389

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, vino a consagrar la relación con las Administraciones públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones.

Con el criterio de que los diarios o boletines oficiales no han de quedar al margen de este nuevo marco general de relación, por vía electrónica, entre los poderes públicos y los ciudadanos, el artículo 11.1 de la citada ley prevé que dichas publicaciones, cuando se realicen en las sedes electrónicas correspondientes, tendrán los mismos efectos que los atribuidos a la edición impresa. Y, en referencia específica al «Boletín Oficial del Estado», la ley dispone que su publicación electrónica «tendrá carácter oficial y auténtico en las condiciones y con las garantías que se determinen reglamentariamente, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables». Esta previsión está sometida a plazo: deberá tener efecto desde el día 1 de enero de 2009, según se determina en la disposición final segunda de la misma ley.

El objetivo principal de este real decreto es dar cumplimiento a ese mandato legal. Ahora bien, el texto de esta nueva norma se inspira en la convicción de que la edición electrónica del Boletín no constituye sólo un paso de alcance meramente tecnológico, que se adopta ante los imperativos de una renovación técnica irreversible. Responde, además, a la conciencia de que la difusión de las normas jurídicas a través de las nuevas redes electrónicas (y muy especialmente por la red «Internet») sitúa la publicación normativa en un plano de accesibilidad y propagación muy superior a todo lo hasta ahora conocido. De ahí la relevancia de conferir a los textos normativos así publicados el carácter oficial y auténtico que durante siglos ha tenido, en exclusiva, su impresión en papel. De esta idea central derivan los contenidos principales de este real decreto.

En primer lugar, se establece el carácter universal y gratuito del acceso a la edición electrónica, y los requerimientos de su aparición diaria en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado.

Se definen, en segundo término, los mecanismos, procesos y demás condiciones y garantías necesarias que aseguren la autenticidad, integridad e inalterabilidad de los contenidos del diario, especialmente a través de la firma electrónica, así como dispositivos para la verificación de tales mecanismos por los propios ciudadanos usuarios de las redes electrónicas.

Igualmente, resulta insoslayable dar cumplimiento eficaz al principio de igualdad consagrado en el artículo 4.b) de la ley, de manera que ningún ciudadano pueda sentirse discriminado por el hecho de no disponer de los medios electrónicos necesarios. Se establecen, para ello, puntos de acceso en oficinas públicas, modalidades varias de apoyo y asistencia a la búsqueda de documentos, así como, en todo caso, la posibilidad, al alcance de todo ciudadano, de obtener una copia impresa en papel de la edición electrónica del Boletín, tanto del ejemplar diario completo como de cada disposición, acto o anuncio en él publicado.

Hay que destacar también que el inicio de la edición electrónica del Boletín no supone la desaparición de la edición impresa, que se mantiene, con el mismo carácter oficial y auténtico, a efectos de conservación y permanencia del diario oficial, y también como medio de difusión en los supuestos en que no resulte posible la aparición de la edición electrónica.

El presente real decreto no se limita a dar carta de naturaleza a la edición electrónica del Boletín Oficial del Estado en nuestra realidad jurídica e institucional. Incorpora, además, parte del Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado, en cuanto se refiere a características, contenido, estructura y procedimiento de publicación, aspectos estos que, en sustancia, resultan aplicables a la edición electrónica, si bien convenientemente renovados en vista de la experiencia de su aplicación y adaptados al nuevo panorama técnico hoy dibujado. En aras de una mayor claridad normativa se ha preferido que la ordenación del diario oficial continúe siendo objeto de una sola norma, lo que supondrá la derogación del Real Decreto hasta ahora vigente.

Se habilita, en fin, al Ministro de la Presidencia para adoptar las medidas y disposiciones necesarias para la ejecución y cumplimiento de lo dispuesto en este real decreto.

En su virtud, a propuesta de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, con la aprobación de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de febrero de 2008,

D I S P O N G O :

CAPÍTULO I

Disposiciones generales

Artículo 1. *Definición.*

El «Boletín Oficial del Estado», diario oficial del Estado español, es el medio de publicación de las leyes, disposiciones y actos de inserción obligatoria.

Artículo 2. *Edición electrónica.*

1. El «Boletín Oficial del Estado» se publica en edición electrónica con arreglo a las condiciones que se establecen en este real decreto, así como en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, y en su normativa de desarrollo.

2. Además de la edición electrónica del «Boletín Oficial del Estado», existirá, obtenida de ésta, una edición impresa con idénticas características y contenido, con la finalidad y en las condiciones previstas en el artículo 13.

Artículo 3. *Carácter oficial y auténtico.*

1. El texto de las leyes, disposiciones y actos publicados en el «Boletín Oficial del Estado» tendrá la consideración de oficial y auténtico, con arreglo a las normas y condiciones que se establecen en este real decreto.

2. El texto de las normas emanadas de las comunidades autónomas que se publiquen en el «Boletín Oficial del Estado» tendrá el carácter que le atribuyan los respectivos Estatutos.

Artículo 4. *Características.*

1. El «Boletín Oficial del Estado» se publicará todos los días del año, salvo los domingos.

2. En la cabecera del ejemplar diario, de cada disposición, acto o anuncio y de cada una de sus páginas figurará:

a) El escudo de España.
b) La denominación «Boletín Oficial del Estado».
c) El número del ejemplar diario, que será correlativo desde el comienzo de cada año.
d) La fecha de publicación.
e) El número de página.

3. En todas y cada una de las páginas se incluirá la dirección de la sede electrónica y el respectivo código de verificación que permitan contrastar su autenticidad, así como acceder a su contenido, en los términos previstos en el artículo 14.4.

4. La fecha de publicación de las disposiciones, actos y anuncios será la que figure en la cabecera y en cada una de las páginas del ejemplar diario en que se inserten.

5. En cada número del diario oficial se incluirá el sumario de su contenido, con indicación del número correlativo que corresponde a cada disposición, acto o anuncio publicado en el mismo.

6. Todas las disposiciones, actos y anuncios abrirán página.

Artículo 5. *Competencias.*

1. Corresponde al Ministerio de la Presidencia, a través de la Secretaría General Técnica-Secretariado del Gobierno la ordenación y control de la publicación de las disposiciones y actos administrativos que deban insertarse en el «Boletín Oficial del Estado», velando especialmente por el orden de prioridad de las inserciones, la salvaguardia de las competencias de los distintos órganos de la Administración y el cumplimiento de los requisitos formales necesarios en cada caso. Podrá también decidir la publicación, en su caso, de números extraordinarios.

2. Corresponde a la Agencia Estatal Boletín Oficial del Estado la edición, publicación y difusión del diario oficial «Boletín Oficial del Estado».

CAPÍTULO II

Contenido del «Boletín Oficial del Estado»

Artículo 6. *Contenido.*

1. En el «Boletín Oficial del Estado» se publicarán:

a) Las disposiciones generales de los órganos del Estado y los tratados o convenios internacionales.

b) Las disposiciones generales de las comunidades autónomas, de acuerdo con lo establecido en los Estatutos de Autonomía y en las normas con rango de ley dictadas para el desarrollo de los mismos.

c) Las resoluciones y actos de los órganos constitucionales del Estado, de acuerdo con lo establecido en sus respectivas leyes orgánicas.

d) Las disposiciones que no sean de carácter general, las resoluciones y actos de los departamentos ministeriales y de otros órganos del Estado y Administraciones públicas, cuando una ley o un real decreto así lo establezcan.

e) Las convocatorias, citaciones, requisitorias y anuncios cuando una ley o un real decreto así lo establezcan.

2. El Consejo de Ministros podrá excepcionalmente acordar la publicación de informes, documentos o comunicaciones oficiales, cuya difusión sea considerada de interés general.

Artículo 7. *Estructura del diario oficial.*

1. El contenido del "Boletín Oficial del Estado" se distribuye en las siguientes secciones:

Sección I: Disposiciones generales.
Sección II: Autoridades y personal.
Sección III: Otras disposiciones.

Sección IV: Administración de Justicia.
Sección V: Anuncios.
Sección del Tribunal Constitucional.

2. Existirán asimismo los siguientes suplementos de carácter independiente:

a) El Suplemento de notificaciones.
b) El Suplemento del Tablón Edictal Judicial Único.

Artículo 8. *Contenido de las secciones y suplementos.*

1. Se incluirán en la sección I:

a) Las leyes orgánicas, las leyes, los reales decretos legislativos y los reales decretos-leyes.
b) Los tratados y convenios internacionales.
c) Las leyes de las asambleas legislativas de las comunidades autónomas.
d) Los reglamentos y demás disposiciones de carácter general.
e) Los reglamentos normativos emanados de los consejos de gobierno de las comunidades autónomas.

2. La sección II estará integrada por dos subsecciones:

a) Nombramientos, situaciones e incidencias.
b) Oposiciones y concursos.

3. La sección III estará integrada por las disposiciones de obligada publicación que no tengan carácter general ni correspondan a las demás secciones.
4. En la sección IV se publicarán:

a) Los anuncios de subastas judiciales.
b) Los actos procesales que no deban ser objeto de inserción en el Suplemento del Tablón Edictal Judicial Único, conforme a lo previsto en el párrafo primero del artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
5. En la sección V se insertarán los anuncios, salvo los de notificación, agrupados de la siguiente forma:

a) Contratación del Sector Público.
b) Otros anuncios oficiales.
c) Anuncios particulares.

6. En la sección del Tribunal Constitucional se publicarán las sentencias, declaraciones y autos del Tribunal Constitucional, en los términos previstos en su ley orgánica.
7. En el Suplemento de notificaciones se insertarán los anuncios de notificación.
8. El Suplemento del Tablón Edictal Judicial Único incluirá las resoluciones y comunicaciones de los Juzgados y Tribunales a las que se refiere el párrafo primero del artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.
Este suplemento estará integrado por dos secciones:

a) Edictos judiciales de carácter general.
b) Edictos judiciales de carácter particular.

Artículo 9. *Estructura de las secciones y subsecciones.*

1. Dentro de cada sección, la inserción de los textos se realizará agrupándolos por el órgano del que procedan, según la ordenación general de precedencias del Estado. Las disposiciones emanadas de las comunidades autónomas se insertarán según el orden de publicación oficial de los Estatutos de Autonomía.
2. Dentro de cada epígrafe, los textos se ordenarán según la jerarquía de las normas.

CAPÍTULO III

Edición electrónica

Artículo 10. *Publicación de la edición electrónica.*

1. La edición electrónica del «Boletín Oficial del Estado» se publicará en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado.

2. La edición electrónica del «Boletín Oficial del Estado» respetará los principios de accesibilidad y usabilidad, de acuerdo con las normas establecidas al respecto, utilizará estándares abiertos y en su caso aquellos otros que sean de uso generalizado por los ciudadanos.

3. La sede electrónica de la Agencia Estatal Boletín Oficial del Estado se dotará de las medidas de seguridad que garanticen la autenticidad e integridad de los contenidos del diario oficial, así como el acceso permanente al mismo, con sujeción a los requisitos establecidos en el Esquema Nacional de Seguridad previsto en el artículo 42 de la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos.

Artículo 11. *Acceso a la edición electrónica.*

1. La Agencia Estatal Boletín Oficial del Estado garantizará, a través de redes abiertas de telecomunicación, el acceso universal y gratuito a la edición electrónica del diario oficial del Estado, sin perjuicio de lo previsto en el artículo 14.4.

2. La edición electrónica del «Boletín Oficial del Estado» deberá estar accesible en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado en la fecha que figure en la cabecera del ejemplar diario, salvo que ello resulte imposible por circunstancias extraordinarias de carácter técnico.

Artículo 12. *Requisitos de la edición electrónica.*

1. La edición electrónica del «Boletín Oficial del Estado» deberá incorporar firma electrónica avanzada como garantía de la autenticidad, integridad e inalterabilidad de su contenido. Los ciudadanos podrán verificar el cumplimiento de estas exigencias mediante aplicaciones estándar o, en su caso, mediante las herramientas informáticas que proporcione la sede electrónica de la Agencia Estatal Boletín Oficial del Estado.

2. Corresponde a la Agencia Estatal Boletín Oficial del Estado:

a) garantizar la autenticidad, integridad e inalterabilidad del diario oficial que se publique en su sede electrónica.

b) custodiar y conservar la edición electrónica del diario oficial del Estado

c) velar por la accesibilidad de la edición electrónica del diario oficial del Estado y su permanente adaptación al progreso tecnológico.

3. La Agencia Estatal Boletín Oficial del Estado publicará en su sede electrónica las prácticas y procedimientos necesarios para la efectividad de lo previsto en este artículo.

Artículo 13. *Garantía de la edición.*

1. La edición impresa del diario oficial tiene las siguientes finalidades:

a) asegurar la publicación del «Boletín Oficial del Estado» cuando por una situación extraordinaria y por motivos de carácter técnico no resulte posible acceder a su edición electrónica;

b) garantizar la conservación y permanencia del diario oficial del Estado y su continuidad como parte del patrimonio documental impreso de la Administración General del Estado.

2. La edición impresa comprenderá los ejemplares necesarios para asegurar la conservación y custodia de al menos tres ejemplares del diario oficial en la Agencia Estatal Boletín Oficial del Estado y en la Secretaría General Técnica-Secretariado del Gobierno, así como los que reglamentariamente se determine para su conservación en la normativa que regula el depósito legal.

3. Los ejemplares de la edición impresa del diario oficial a los que se refiere el apartado anterior, serán realizados, conservados y custodiados de manera que quede garantizada su perdurabilidad.

4. No obstante lo dispuesto en los apartados anteriores, los suplementos de notificaciones y del Tablón Edictal Judicial Único solamente contarán con edición impresa cuando concurran las circunstancias previstas en la letra a) del apartado primero.

CAPÍTULO IV

Acceso de los ciudadanos al «Boletín Oficial del Estado»

Artículo 14. *Acceso de los ciudadanos.*

1. Los ciudadanos tendrán acceso libre y gratuito a la edición electrónica del «Boletín Oficial del Estado». Dicho acceso comprenderá la posibilidad de búsqueda y consulta del contenido del diario, así como la posibilidad de archivo e impresión, tanto del diario completo como de cada una de las disposiciones, actos o anuncios que lo componen.

2. En todas las oficinas de información y atención al ciudadano de la Administración General del Estado, se facilitará la consulta pública y gratuita de la edición electrónica del «Boletín Oficial del Estado. Con ese fin, en cada una de estas oficinas existirá al menos un terminal informático, a través del cual se podrán realizar búsquedas y consultas del contenido del diario. Las mencionadas oficinas deberán facilitar a las personas que lo soliciten una copia impresa de las disposiciones, actos o anuncios que requieran, o del diario completo, mediante, en su caso, la contraprestación que proceda.

3. Mediante orden del Ministro de la Presidencia podrán establecerse las condiciones de obtención de copias auténticas impresas de las disposiciones, actos o anuncios o del diario completo, tanto en la Agencia Estatal Boletín Oficial del Estado, como en las oficinas públicas de consulta.

4. No obstante lo previsto en los apartados anteriores, los suplementos permanecerán libremente accesibles en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado durante un plazo de tres meses, en el caso del Suplemento de notificaciones, y de cuatro meses, en el caso del Suplemento del Tablón Edictal Judicial Único.

Una vez transcurrido el plazo correspondiente a cada suplemento, el acceso requerirá el código de verificación del correspondiente documento, que tendrá carácter único y no previsible.

(Párrafo anulado)

La Agencia Estatal Boletín Oficial del Estado adoptará medidas orientadas a evitar la indexación y recuperación automática de la información publicada en los suplementos por parte de sujetos distintos a los contemplados en el párrafo anterior.

Sin perjuicio de lo previsto en las disposiciones adicionales primera y cuarta, finalizados los plazos previstos, respectivamente, en el párrafo primero de este apartado, la Agencia Estatal Boletín Oficial del Estado facilitará el documento publicado, previa solicitud, únicamente a los interesados o a sus representantes, al Ministerio Fiscal, al Defensor del Pueblo, y a los Juzgados y Tribunales.

Téngase en cuenta que se declara la nulidad del párrafo tercero del apartado 4, en la redacción dada por el art. único.4 del Real Decreto 327/2021, de 11 de mayo, por Sentencia del TS de 5 de julio de 2022, en los términos de su fundamento de derecho quinto. Ref. BOE-A-2022-15542

Redacción anterior:

"4. No obstante lo previsto en los apartados anteriores, el Suplemento de notificaciones permanecerá libremente accesible en la sede electrónica de la Agencia Estatal Boletín Oficial del Estado durante un plazo de tres meses desde su publicación, transcurrido el cual se requerirá el código de verificación del correspondiente anuncio de notificación, que tendrá carácter único y no previsible.

Dicho código solamente podrá ser conservado, almacenado y tratado por el interesado o su representante, así como por los órganos y Administraciones que puedan precisarlo para el ejercicio de las competencias que les corresponden.

La Agencia Estatal Boletín Oficial del Estado adoptará medidas orientadas a evitar la indexación y recuperación automática de los códigos de verificación por sujetos distintos a los contemplados en el párrafo anterior.

Sin perjuicio de lo previsto en la disposición adicional primera, una vez transcurrido el plazo de tres meses establecido en el párrafo primero, la Agencia Estatal Boletín Oficial del Estado facilitará, previa solicitud, la información contenida en el anuncio de notificación únicamente al interesado o su representante, al Ministerio Fiscal, al Defensor del Pueblo, y a los Jueces y Tribunales."

Artículo 15. *Servicio de ayuda.*

La Agencia Estatal Boletín Oficial del Estado ofrecerá un servicio gratuito de asistencia a los ciudadanos en la búsqueda de las disposiciones, actos y anuncios publicados en el diario oficial y les facilitará, cuando así lo soliciten, una copia impresa de aquéllas, o del diario completo, mediante la correspondiente contraprestación que reglamentariamente se establezca.

Se exceptúan de lo previsto en el párrafo anterior los documentos publicados en los suplementos de notificaciones y del Tablón Edictal Judicial Único, una vez hayan transcurrido los plazos previstos, respectivamente, en el apartado cuatro del artículo 14.

Artículo 16. *Convenios con otras Administraciones públicas.*

Se celebrarán convenios con las comunidades autónomas, las administraciones locales, las universidades y otros entes públicos para que ofrezcan los servicios a los que se refieren los artículos 14 y 15.

Artículo 17. *Servicio de base de datos.*

La Agencia Estatal Boletín Oficial del Estado ofrecerá en su sede electrónica, con carácter diferenciado a la edición electrónica del ‘‘Boletín Oficial del Estado’’, una base de datos gratuita que permita la búsqueda, recuperación e impresión de las disposiciones, actos y anuncios publicados en el ‘‘Boletín Oficial del Estado’’, con sujeción a lo establecido en la normativa de protección de datos personales.

No obstante, la búsqueda, recuperación e impresión, a través del servicio de base de datos, de los documentos publicados en los suplementos de notificaciones y del Tablón Edictal Judicial Único, será posible exclusivamente durante los plazos previstos, respectivamente, en el apartado cuatro del artículo 14.

Artículo 18. *Accesibilidad.*

La edición electrónica del diario oficial tendrá las condiciones de accesibilidad necesarias para su consulta por las personas con discapacidad o de edad avanzada.

CAPÍTULO V

Procedimiento de publicación

Artículo 19. *Facultad de ordenar la inserción.*

1. La inserción en el diario oficial del Estado de las leyes aprobadas por las Cortes Generales se hará del modo previsto en el artículo 91 de la Constitución.

2. La facultad de ordenar la inserción de los reales decretos-leyes corresponde al Ministro que ejerza la secretaría del Consejo de Ministros. La de los reales decretos legislativos y los reales decretos, al ministro que los refrende o, por su delegación, a los demás órganos superiores del departamento correspondiente.

3. La facultad de ordenar la inserción de las restantes disposiciones y actos queda atribuida del siguiente modo:

a) En los departamentos ministeriales, a los Ministros, Secretarios de Estado en el ámbito de su competencia, Subsecretarios, Secretarios Generales Técnicos y los Directores Generales o equivalentes. Cuando se trate de normas o actos dictados a propuesta de varios departamentos, la publicación será ordenada por los correspondientes órganos del Ministerio de la Presidencia.

b) Las disposiciones y actos emanados de los órganos constitucionales del Estado y de otras Administraciones Públicas, a las autoridades que tengan atribuida la representación de cada órgano o Administración o a aquellos en los que se delegue expresamente.

4. La facultad de ordenar la inserción de los anuncios u otros actos que deban publicarse en las Secciones IV y V del Boletín Oficial del Estado, la tendrán las autoridades que en los órganos constitucionales del Estado o en cada Administración o entidad tengan atribuida la competencia o estén autorizados para ello.

5. La facultad de ordenar la inserción de los anuncios de notificación que deban publicarse en el Suplemento de notificaciones corresponde a los órganos que en cada Administración o entidad, tengan atribuida dicha competencia o estén autorizados para ello, así como a los órganos que hayan emitido los correspondientes anuncios.

6. La facultad de ordenar la inserción de los actos procesales que deban publicarse en el Suplemento del Tablón Edictal Judicial Único corresponde a los Juzgados y Tribunales en los términos previstos por las normas procesales.

Artículo 20. *Remisión de documentos.*

1. Los originales destinados a la publicación en las secciones I, II, III y del Tribunal Constitucional se remitirán en formato electrónico, de acuerdo con las garantías, especificaciones y modelos que para cada órgano y Administración se establezcan mediante orden del Ministro de la Presidencia y que figuren en las sedes electrónicas del Ministerio de la Presidencia y de la Agencia Estatal Boletín Oficial del Estado.

2. Los originales destinados a la publicación en las secciones IV y V se remitirán en formato electrónico, de acuerdo con las garantías, especificaciones y modelos que se establezcan mediante resolución de la Agencia Estatal Boletín Oficial del Estado, publicada en su sede electrónica.

3. Los originales destinados a la publicación en el Suplemento de notificaciones se remitirán mediante el sistema automatizado de remisión y gestión telemática previsto en la disposición adicional tercera de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, de acuerdo con las garantías, especificaciones básicas y modelos que se establecen en la disposición adicional primera de este real decreto.

4. Los originales destinados a la publicación en el Suplemento del Tablón Edictal Judicial Único se remitirán mediante el sistema automatizado de remisión y gestión telemática previsto en el artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, de acuerdo con las garantías, especificaciones básicas y modelos que se establecen en la disposición adicional cuarta de este real decreto.

5. En todo caso, el formato de los documentos, ya sea de texto, gráfico, de imagen o cualquier otro, deberá atender los estándares que garanticen el adecuado nivel de interoperabilidad y resultar idóneo para comunicar el contenido del documento de que se trate.

Artículo 21. *Autenticidad de los documentos.*

1. Respecto a las disposiciones y actos de las secciones I, II, III y del Tribunal Constitucional, se aplicarán las siguientes normas:

a) La autenticidad de los originales remitidos para publicación habrá de quedar garantizada mediante su firma electrónica, de conformidad con lo que prevea la orden del Ministro de la Presidencia a la que se refiere el artículo 20.

b) A tal efecto, en la Secretaría General Técnica-Secretariado del Gobierno existirán los registros de firmas electrónicas de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

c) En cada departamento ministerial, el Subsecretario determinará las tres autoridades o funcionarios que, además de los titulares de los órganos superiores, estarán facultados para firmar la inserción de los originales destinados a publicación.

d) Los órganos constitucionales y las Administraciones públicas, de acuerdo con su normativa específica, determinarán las autoridades o funcionarios facultados para firmar la inserción de originales, sin que el número de firmas reconocidas pueda exceder de tres por cada órgano o Administración.

e) La autoridad o funcionario que suscriba la inserción de los originales se hará responsable de la autenticidad de su contenido y de la existencia de la correspondiente orden de inserción adoptada en los términos a los que se refiere el artículo 19.

2. Respecto a los anuncios y otros actos de las secciones IV y V, la Agencia Estatal Boletín Oficial del Estado mantendrá un registro de las entidades y organismos firmantes de los anuncios que se publiquen en el diario oficial. La autenticidad de los originales remitidos para publicación deberá quedar garantizada mediante alguno de los sistemas de firma electrónica previstos en el artículo 13 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

3. Respecto de los anuncios de notificación que se publiquen en el Suplemento de notificaciones, la autenticidad de los originales remitidos para publicación deberá quedar garantizada en los términos previstos en la disposición adicional primera.

4. Respecto de los documentos que se publiquen en el Suplemento del Tablón Edictal Judicial Único, la autenticidad de los originales remitidos para publicación deberá quedar garantizada en los términos previstos en la disposición adicional cuarta.

Artículo 22. *Competencia en relación con las diversas secciones.*

1. Los textos de las disposiciones, resoluciones, sentencias y actos incluidos en las secciones I, II, III y del Tribunal Constitucional serán remitidos, en todo caso, a la Secretaría General Técnica-Secretariado del Gobierno, que procederá a la clasificación de los mismos y a la comprobación de la autenticidad de las firmas, velando especialmente por el orden de prioridad de las inserciones, la salvaguarda de las competencias de los distintos órganos de la Administración, la obligatoriedad de la inserción y el cumplimiento de los requisitos formales necesarios en cada caso.

2. Los originales de los anuncios y otros actos que deban insertarse en las secciones IV y V se remitirán directamente por los organismos, entidades y personas interesadas a la Agencia Estatal Boletín Oficial del Estado o, en su caso, a través de la Plataforma de Contratación del Sector Público.

3. Los anuncios de notificación se remitirán a la Agencia Estatal Boletín Oficial del Estado, en los términos previstos en las disposiciones adicionales primera y segunda.

4. Los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único, se remitirán a la Agencia Estatal Boletín Oficial del Estado en los términos previstos en la disposición adicional cuarta.

Artículo 23. *Tramitación de la documentación.*

1. Los originales recibidos para publicación en el «Boletín Oficial del Estado» tendrán carácter reservado y no podrá facilitarse información acerca de ellos.

2. Los originales serán insertados en los mismos términos en que se hallen redactados y autorizados, sin que puedan modificarse, salvo autorización del organismo remitente.

Artículo 24. *Publicación íntegra y en extracto.*

1. Las disposiciones, resoluciones, sentencias y actos incluidos en la sección I y en la sección del Tribunal Constitucional se publicarán en forma íntegra.

2. Las resoluciones y actos comprendidos en las secciones II, III, IV y V, así como en el Suplemento de notificaciones, se publicarán en extracto, siempre que sea posible y se reúnan los requisitos exigidos en cada caso.

Los actos procesales objeto de inserción en el Suplemento del Tablón Edictal Judicial Único se publicarán en extracto, en los términos establecidos por las normas procesales. En todo caso, deberán quedar salvaguardados los derechos e intereses de los menores, así como otros derechos y libertades que pudieran verse afectados por la publicación.

3. Los organismos remitentes enviarán debidamente extractados los textos y documentos susceptibles de ser publicados en esta forma.

Artículo 25. *Justificación de la obligatoriedad de la inserción.*

Cuando se susciten dudas sobre la procedencia de publicar una determinada disposición o texto, el organismo remitente hará constar en su escrito la norma en la que se establezca la obligatoriedad de la inserción.

Artículo 26. *Correcciones.*

Si alguna disposición oficial aparece publicada con errores que alteren o modifiquen su contenido, será reproducida inmediatamente en su totalidad o en la parte necesaria, con las debidas correcciones. Estas rectificaciones se realizarán de acuerdo con las siguientes normas:

a) Se corregirán de oficio las erratas padecidas en la publicación, siempre que supongan alteración o modificación del sentido de las mismas o puedan suscitar dudas al respecto. A tal efecto, los correspondientes servicios de la Secretaría General Técnica-Secretariado del Gobierno y de la Agencia Estatal Boletín Oficial del Estado, conservarán los originales de cada número, durante el plazo de tres meses, a partir de la fecha de su publicación.

b) Cuando se trate de errores padecidos en el texto recibido en la Agencia Estatal Boletín Oficial del Estado para publicación, su rectificación se realizará del modo siguiente:

1.º Los meros errores u omisiones materiales, que no constituyan modificación o alteración del sentido de las disposiciones o se deduzcan claramente del contexto, pero cuya rectificación se juzgue conveniente para evitar posibles confusiones, se salvarán por los organismos respectivos instando la reproducción del texto, o de la parte necesaria del mismo, con las debidas correcciones.

2.º En los demás casos, y siempre que los errores u omisiones puedan suponer una real o aparente modificación del contenido o del sentido de la norma, se salvarán mediante disposición del mismo rango.

Artículo 27. *Inserciones gratuitas y de pago.*

1. La publicación de las leyes, disposiciones, resoluciones, sentencias y actos de inserción obligatoria que deban ser incluidos en las secciones I, II, III y del Tribunal Constitucional, se efectuará sin contraprestación económica por parte de los órganos que la hayan interesado.

2. La publicación de anuncios en las secciones IV y V está sujeta al pago de la correspondiente tasa, de acuerdo con lo dispuesto en la Ley 25/1998, de 13 de julio, de modificación del régimen legal de las tasas estatales y de reordenación de las prestaciones patrimoniales de carácter público y en el Estatuto de la Agencia Estatal Boletín Oficial del Estado, aprobado por Real Decreto 1495/2007, de 12 de noviembre.

3. La publicación de documentos en los suplementos de notificaciones y del Tablón Edictal Judicial Único se efectuará sin contraprestación económica alguna por parte de los organismos que la hayan interesado.

Disposición adicional primera. *Sistema automatizado de remisión y gestión telemática de los anuncios de notificación.*

1. El sistema automatizado de remisión y gestión telemática de la Agencia Estatal Boletín Oficial del Estado, para la publicación de los anuncios de notificación, previsto en la disposición adicional vigésima primera de la Ley 30/1992, de 26 de noviembre, deberá ajustarse a las siguientes garantías y especificaciones básicas:

a) El acceso al sistema requerirá previa identificación, que podrá realizarse mediante DNI electrónico o certificado electrónico reconocido. Asimismo, podrá requerirse estar dado de alta en el repositorio horizontal de usuarios de las Administraciones Públicas. En caso de que el acceso se realice mediante servicios web, se podrá utilizar el sistema de firma electrónica mediante sello electrónico del correspondiente órgano, entidad o Administración.

Cada Administración Pública o entidad determinará, de acuerdo con su normativa específica, las autoridades o empleados públicos autorizados. En el caso de las entidades locales, la autorización inicial deberá ser comunicada telemáticamente a la Agencia Estatal Boletín Oficial del Estado por un funcionario de Administración local con habilitación de carácter nacional.

b) Las Administraciones y entidades usuarias estarán obligadas a mantener permanentemente actualizado el catálogo de unidades administrativas implicadas en el procedimiento de publicación, mediante el directorio común a que se refiere el artículo 9 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.

c) La remisión se realizará preferentemente mediante servicios web conforme al formato estructurado que se contiene en el anexo de este real decreto, el cual podrá ser actualizado mediante resolución de la Agencia Estatal Boletín Oficial del Estado. Asimismo, la remisión podrá realizarse por medio de un portal web. En todo caso, deberán incorporarse los metadatos que permitan la gestión automatizada de los documentos por parte de la Agencia Estatal Boletín Oficial del Estado.

d) El sistema de remisión garantizará la autenticidad, integridad y no repudio de los envíos, así como su confidencialidad.

e) El sistema permitirá consultar, mediante servicios web u otros mecanismos, el estado de tramitación de los anuncios de notificación enviados, así como acceder a su publicación sin limitación temporal alguna, en los términos que cada Administración Pública o entidad haya autorizado, conforme a lo previsto en la letra a) de este apartado.

f) Los anuncios de notificación serán publicados dentro de los tres días hábiles siguientes a su recepción, salvo los supuestos de imposibilidad técnica, solicitud de un plazo de publicación superior por el órgano remitente o que el anuncio de notificación requiera de subsanación. A estos efectos, los anuncios de notificación recibidos después de las 12:00 horas del viernes, los sábados, días festivos y 24 y 31 de diciembre se considerarán recibidos a las 8:00 horas del primer día hábil siguiente.

2. Corresponde a la Agencia Estatal Boletín Oficial del Estado determinar los requisitos y las especificaciones técnicas del sistema, que, en todo caso, deberá cumplir con lo establecido en la Ley 11/2007, de 22 de junio, y su normativa de desarrollo.

Disposición adicional segunda. *Anuncios de notificación en procedimientos sancionadores en materia de tráfico.*

(Derogada)

Disposición adicional tercera. *Remisión telemática de documentos a publicar en las secciones I, II, III y del Tribunal Constitucional.*

Las garantías, especificaciones y modelos a los que se refiere el artículo 20.1 son los previstos en las Ordenes PRE/1563/2006, de 19 de mayo, por la que se regula el procedimiento para la remisión telemática de las disposiciones y actos administrativos de los departamentos ministeriales que deban publicarse en el "Boletín Oficial del Estado" y PRE/987/2008, de 8 de abril, por la que se amplía su ámbito de aplicación, para los departamentos ministeriales, órganos y entidades previstos en sus respectivos ámbitos de aplicación.

Disposición adicional cuarta. *Sistema automatizado de remisión y gestión telemática de los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único.*

1. El sistema automatizado de remisión y gestión telemática de la Agencia Estatal Boletín Oficial del Estado, previsto en el artículo 35 de la Ley 18/2011, de 5 de julio, reguladora del

uso de las tecnologías de la información y la comunicación en la Administración de Justicia, se ajustará a las siguientes garantías y especificaciones básicas:

a) El acceso al sistema requerirá previa identificación de los funcionarios al servicio del órgano judicial competente, que podrá realizarse mediante DNI electrónico u otro certificado electrónico cualificado. En caso de que el acceso se realice mediante servicios web, se deberá utilizar el sistema de firma electrónica mediante sello electrónico cualificado del correspondiente sistema de gestión procesal.

b) El Ministerio de Justicia mantendrá permanentemente actualizado y accesible mediante servicios web, el catálogo de órganos judiciales y de usuarios implicados en el procedimiento de publicación y el Ministerio de Defensa, respecto de los órganos judiciales militares.

c) La remisión se realizará preferentemente mediante servicios web conforme al formato estructurado que se contiene en el anexo II de este real decreto. Asimismo, la remisión podrá realizarse por medio de un portal web. En todo caso, deberán incorporarse los metadatos que permitan la gestión automatizada de los documentos por parte de la Agencia Estatal Boletín Oficial del Estado.

d) El sistema de remisión garantizará la autenticidad, integridad y no repudio de los envíos, así como su confidencialidad.

e) El sistema permitirá consultar, mediante servicios web u otros mecanismos, el estado de tramitación de los documentos enviados, así como acceder a su publicación sin limitación temporal alguna, conforme a lo previsto en la letra a) de este apartado.

f) Los documentos serán publicados dentro de los tres días hábiles siguientes a su recepción, salvo los supuestos de imposibilidad técnica, solicitud de un plazo de publicación superior por el remitente o que el documento requiera de subsanación. A estos efectos, los documentos recibidos después de las 12:00 horas del viernes, los sábados, días festivos y 24 y 31 de diciembre se considerarán recibidos a las 8:00 horas del primer día hábil siguiente.

2. Corresponde a la Dirección de la Agencia Estatal Boletín Oficial del Estado determinar los requisitos y las especificaciones técnicas del sistema.

Disposición transitoria única. *Remisión de documentos a publicar en las secciones I, II, III y del Tribunal Constitucional.*

En tanto no se aprueben las garantías, especificaciones y modelos para los órganos y Administraciones no contemplados en el ámbito de aplicación de las Órdenes PRE/1563/2006, de 19 de mayo, y PRE/987/2008, de 8 de abril, continuarán remitiéndose los originales a publicar en formato papel, con firma manuscrita de quien esté facultado al efecto, acompañados de los ficheros electrónicos a partir de los cuales se generaron los originales remitidos y ajustándose en todas sus características a los modelos oficiales que figuran en las sedes electrónicas del Ministerio de la Presidencia y de la Agencia Estatal Boletín Oficial del Estado.

A estos efectos, la Secretaría General Técnica-Secretariado del Gobierno mantendrá un registro de firmas manuscritas de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

Disposición derogatoria única. *Derogación normativa.*

1. Queda derogado el Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado.

2. Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Habilitación normativa.*

1. Se autoriza al Ministro de la Presidencia para que dicte cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en este real decreto, y en particular para el establecimiento de las garantías y especificaciones con arreglo a las cuales los originales destinados a la publicación en el «Boletín Oficial del Estado» podrán remitirse a

través de medios electrónicos, informáticos y telemáticos, así como para el establecimiento de los modelos electrónicos que deban emplearse para la remisión telemática de los originales de disposiciones o actos que deban ser insertados en el «Boletín Oficial del Estado».

2. Los anexos I y II podrán ser actualizados mediante resolución de la Dirección de la Agencia Estatal Boletín Oficial del Estado, que deberá publicarse en el "Boletín Oficial del Estado".

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día 1 de enero de 2009.

ANEXO I

Formato XML para el envío de anuncios de notificación

El contenido del envío se realizará en formato XML con la información estructurada de la siguiente forma:

```
<envio>
    <version>
    <anuncios>
        <remitente>
            <nodoRemitente +>
        </remitente>
        <fechaPub ?>
        <infPub>
            <urlSW ?>
            <email>
        </infPub>
        <anuncio +>
            <emisor>
                <nodoEmisor +>
            </emisor>
            <metadatos>
                <id ?>
                <formPub>
                <datosPersonales>
                <lgt ?>
                <procedimiento ?>
                <materias ?>
                    <materia +>
                </materias>
                <notificados ?>
                    <notificado +>
                </notificados>
            </metadatos>
            <contenido>
                <texto>
                    <p +>
                    <table *>
                </texto>
                <pieFirma>
                    <lugar>
                    <fecha>
                    <firmante>
                </pieFirma>
            </contenido>
            <contenidoCoof ?>
                <texto>
                    <p +>
                    <table *>
                </texto>
            </contenidoCoof>
        </anuncio>
    </anuncios>
</envio>
```

```
+ significa una o más ocurrencias
? significa cero o una ocurrencia
* significa cero o más ocurrencias
```

En la descripción de los contenidos del fichero XML se hace referencia a una serie de tipos de datos por su acrónimo. A continuación se enumeran estos tipos de datos.

NIF: Número de Identificación Fiscal. Deberá proporcionarse siempre justificado con «0» a la izquierda, sin puntos, ni espacios, ni guiones ni ningún otro carácter distinto de un número o una letra.

NAF: Número de afiliación a la Seguridad Social.

CCC: Código de cuenta de cotización.

EXP: Número de expediente.

DIR3: Directorio común de Unidades orgánicas y oficinas. La descripción de este servicio se encuentra en el PAE (portal de administración electrónica) en la siguiente URL: http://administracionelectronica.gob.es/ctt/dir3.

La Agencia Estatal Boletín Oficial del Estado pondrá asimismo en su sede electrónica el fichero XSD (XML Schema Definition) para la validación previa al envío de los ficheros XML con el contenido de los anuncios, la documentación del servicio web para el envío de dichos ficheros y ejemplos de ficheros XML con distintos tipos de notificaciones.

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
	envio	Nodo raíz del envío		[1..1]	
1	version	Código que indica la versión utilizada. Existirá compatibilidad de versiones.	[1.0.0]	[1..1]	string
2	anuncios			[1..1]	complexType
2.1	remitente	Organismo o unidad remitente de los anuncios. Contiene el árbol de la estructura del directorio DIR3 del organismo o unidad, incluyendo un elemento nodoRemitente para cada nivel en DIR3.		[1..1]	complexType
2.1.1	nodoRemitente	Organismo o unidad remitente de los anuncios. Contiene dos atributos: idDir3: Código DIR3 del organismo. Tipo dato: string. nivel: Nivel dentro del árbol conforme a la estructura DIR3. Tipo dato: int. Por ejemplo, en el caso de la Agencia Estatal Boletín Oficial del Estado sería: <nodoRemitente nivel="1" idDir3="EA9999999">ADMINISTRACIÓN GENERAL DEL ESTADO</nodoRemitente> <nodoRemitente nivel="2" idDir3="E00004101">MINISTERIO DE LA PRESIDENCIA</nodoRemitente> <nodoRemitente nivel="3" idDir3="E00135501">SUBSECRETARIA DE LA PRESIDENCIA</nodoRemitente> <nodoRemitente nivel="4" idDir3="E04761001">AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO</nodoRemitente>		[1..*]	string
2.2	fechaPub	Fecha de publicación solicitada para los anuncios. Si la fecha se correspondiese con un domingo, la publicación se realizará el lunes siguiente. Si no se incluye o es incorrecta se procederá a publicar en la fecha más temprana posible conforme al procedimiento de cierre y publicación que rige la publicación del BOE. La fecha se especificará en formato ISO 8601:2004 (aaaa-mm-dd). Por ejemplo: <fechaPub>2015-11-01</fechaPub> Nota: El BOE se publica todos los días del año con la única excepción de los domingos.		[0..1]	date
2.3	infPub	Contendrá la dirección del servicio web del órgano emisor al que se informará de la fecha de publicación de los anuncios y una dirección de correo electrónico. La forma de comunicar dicha información se tratará en documento aparte.		[1..1]	complexType
2.3.1	urlSW	Dirección del servicio web a la que se informará de la fecha de publicación de los anuncios.		[0..1]	anyUri
2.3.2	email	Dirección de correo electrónico a efectos de comunicar las incidencias que se generen en el proceso de la información.		[1..1]	string
2.4	anuncio	Este elemento puede repetirse ya que se admiten envíos con más de un anuncio. Cada elemento representará un anuncio distinto.		[1..*]	complexType
2.4.1	emisor	Organismo o unidad autor del anuncio. Contiene el árbol de la estructura del directorio DIR3 del organismo o unidad, incluyendo un elemento nodoEmisor para cada nivel. Nota: El organismo o unidad autor del anuncio no tiene que coincidir necesariamente con el remitente		[1..1]	complexType
2.4.1.1	nodoEmisor	Organismo o unidad autor del anuncio. Contiene dos atributos: idDir3: Código DIR3 del organismo. Tipo dato: string. nivel: Nivel dentro del árbol conforme a la estructura DIR3. Tipo dato: int. Por ejemplo, en el caso de la Agencia Estatal Boletín Oficial del Estado sería: <nodoEmisor nivel="1" idDir3="EA9999999">ADMINISTRACIÓN GENERAL DEL ESTADO</nodoEmisor> <nodoEmisor nivel="2" idDir3="E00004101">MINISTERIO DE LA PRESIDENCIA</nodoEmisor> <nodoEmisor nivel="3" idDir3="E00135501">SUBSECRETARIA DE LA PRESIDENCIA</nodoEmisor> <nodoEmisor nivel="4" idDir3="E04761001">AGENCIA ESTATAL BOLETIN OFICIAL DEL ESTADO</nodoEmisor>		[1..*]	string
2.4.2	metadatos	Información que no se publicará pero indispensable para el tratamiento de los anuncios y la forma de publicarlos.		[1..1]	complexType
2.4.2.1	id	Identificador único del anuncio en los sistemas de información del órgano emisor. Aunque no es obligatorio, es indispensable para que se pueda informar al emisor de la fecha de publicación del anuncio. Es necesario si se ha incluido el elemento infPub/urlSW. Nota: Si no se ha proporcionado el dato y el elemento infPub/urlSW fue proporcionado se devolverá un aviso tras la recepción del XML pero no se detendrá la publicación. No será posible utilizar el servicio de Control de Publicación.		[0..1]	string

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
2.4.2.2	formPub	Forma de publicación. Es un dato obligatorio imprescindible para el tratamiento posterior y la forma de mostrar el anuncio. Puede tomar dos valores: E: Publicación en extracto (cuando el anuncio no contiene el contenido del acto administrativo a notificar, sino únicamente la identificación del interesado y del procedimiento) I: Publicación íntegra (cuando en el texto del anuncio se recoge completo el contenido del acto administrativo objeto de notificación)	[E],[I]	[1..1]	string
2.4.2.3	datosPersonales	Informa sobre si el anuncio contiene datos de carácter personal. Puede tomar los siguientes valores: N: No incluye ningún dato de carácter personal. S: Incluye datos de carácter personal.	[N],[S]	[1..1]	string
2.4.2.4	materias	Tipo de anuncio. Por ejemplo: "catastro", "impuestos", "tasas", "subvenciones" con el objetivo de facilitar la recuperación posterior en base de datos. Contendrá tantos elementos "materia" como sean precisos para facilitar la búsqueda del anuncio. Clasificación a determinar.		[0..1]	complexType
2.4.2.4.1	materia	Materia. Incluye el atributo idMat (tipo de datos string) con el identificador de la materia. Ejemplo: <materia idMat="12">tasas</materia> <materia idMat="23">catastro</materia>		[1..*]	string
2.4.2.5	lgt	El valor será "S" si el anuncio debe publicarse conforme a lo dispuesto en el artículo 112 de la Ley 58/2003 (Ley General Tributaria).	[S]	[0..1]	string
2.4.2.6	procedimiento	Identificación del procedimiento. Es un texto libre que permitirá construir de manera automatizada el título del anuncio y diferenciar entre los emitidos en igual fecha por el mismo emisor. Asimismo, una vez publicado el anuncio, facilitará la búsqueda por texto libre. Deberá incluir un atributo "plural" para indicar si debe emplearse el plural en la palabra procedimiento en el momento de generar el título del anuncio; para ello tomará el valor "S" para indicar el plural y "N" el singular. Se admitirá un máximo de 400 caracteres. No debe contener datos de carácter personal. Ejemplos (en primer lugar el bloque XML y a continuación el título del anuncio al que daría lugar): Ejemplo 1: <procedimiento plural="N">sancionador</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento sancionador Ejemplo 2: empleo del plural. En este ejemplo se incluye además un órgano que tramita el procedimiento. Este órgano debe ser un órgano distinto al emisor): <procedimiento plural="S"> tramitados por la Subdirección de.../departamento/Servicio de...</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimientos tramitados por la Subdirección de.../departamento/Servicio de... Ejemplo 3: <procedimiento plural="N"> nº de expediente xxx</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento nº de expediente xxx Ejemplo 4: <procedimiento plural="N"> de concesión de las subvenciones previstas en la Orden xxx, por la que se aprueban las correspondientes bases reguladoras</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento de concesión de las subvenciones previstas en la Orden xxx, por la que se aprueban las correspondientes bases reguladoras. Ejemplo 5: <procedimiento plural="N"> relativo a baja en el padrón municipal</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento relativo a baja en el padrón municipal Ejemplo 6 (correcciones de errores): <procedimiento plural="N"> relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores Ejemplo 7 (correcciones de errores): <procedimiento plural="N"> relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores del anuncio de notificación de 19 de julio</procedimiento> Anuncio de notificación de 23 de julio de 2014, en procedimiento relativo a liquidaciones del Impuesto sobre Bienes Inmuebles. Corrección de errores del anuncio de notificación de 19 de julio.		[0..1]	string
2.4.2.7	notificados	Aunque el elemento es opcional, deberá incluirse aquí la lista con los datos de los notificados si no es posible marcarlos en el elemento contenido/texto que se describe en el punto siguiente. Contendrá tantos elementos "notificado" como notificados haya.		[0..1]	complexType
2.4.2.7.1	notificado	Cada elemento notificado incluirá obligatoriamente el atributo id (tipo de dato string) que contendrá su identificación (normalmente el NIF) y el atributo tipId (tipo de dato string) para el tipo de identificador (NIF, NAF, CCC, EXP). Ejemplo: <notificado id="99999999R" tipId="NIF">Juan Español Español</notificado>		[1..*]	string
2.4.2.8	contenido	Contenido del anuncio.			complexType
2.4.2.8.1	texto	Texto del anuncio. Incluirá de forma obligatoria un atributo content-type (tipo de dato string) con el valor "application/xml" El nodo texto estará formado por dos tipos de nodos que pueden repetirse tantas veces como sea necesario: párrafos (p) y tablas (table). El anuncio debe contener al menos un elemento párrafo.		[1..1]	complexType
2.4.2.8.1.1	p	Párrafo de texto. Puede admitir un atributo class (tipo de dato string) para presentar la información. Este atributo puede tomar los siguientes valores: parrafo: Párrafo por defecto. titulo: Párrafo centrado con un tipo de letra mayor que el del párrafo por defecto. pieFirma: El elemento no tendrá contenido alguno. Representa la posición donde se incorporá el texto del elemento pieFirma. De no incluirse, el pie de firma irá al final del texto. page-break: El elemento no tendrá contenido alguno. Fuerza un salto de página a partir de este elemento. Si no se indica el atributo, se le aplicará el atributo del párrafo por defecto. Ejemplos: Este es un párrafo normal Este es otro párrafo normal ANEXO		[1..*]	string

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
2.4.2.8.1.1.1	span	Dentro de un párrafo se podrán incluir elementos span con el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC, EXP o un nombre, para marcar un contenido a indexar si este no se ha incluido en el apartado metadatos/notificados. Por ejemplo: Se notifica a Juan Español Español con NIF 99999999R lo siguiente....			string
2.4.2.8.1.2	table	Tabla con información		[0..*]	complexType
2.4.2.8.1.2.1	caption	Título de la tabla		[0..1]	string
2.4.2.8.1.2.2	colgroup	Contiene información de las columnas de la tabla. Debe contener tantos elementos col como columnas tenga la tabla.		[0..1]	complexType
2.4.2.8.1.2.2.1	col	En él podrá especificarse si el contenido de la columna deberá ser indexado e incorporado al buscador añadiéndole el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC o un nombre. Ejemplo: <colgroup> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col /> <col /> <col /> </colgroup> En este ejemplo las columnas 1 y 3 de la tabla incluyen un NIF y las 2 y 4 un NOMBRE que deben incorporarse al buscador. Las columnas 5, 6 y 7 no se incorporarán al buscador.		[1..*]	complexType
2.4.2.8.1.2.3	thead	Cabecera de la tabla.		[0..1]	complexType
2.4.2.8.1.2.3.1	tr	Fila de la cabecera		[1..*]	complexType
2.4.2.8.1.2.3.1.1	th	Celda de la cabecera. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.8.1.2.4	tbody	Cuerpo de la tabla.		[1..1]	complexType
2.4.2.8.1.2.4.1	tr	Fila de la tabla		[1..*]	complexType
2.4.2.8.1.2.4.1.1	td	Celda de la tabla. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.8.1.2.5	tfoot	Pie de la tabla. Normalmente no se usará.		[0..1]	complexType
2.4.2.8.1.2.5.1	tr	Fila del pie		[1..*]	complexType
2.4.2.8.1.2.5.1.1	th	Celda del pie. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.8.2	pieFirma	Pie de firma del anuncio Ejemplo 1: <pieFirma> <lugar>Madrid</lugar> <fecha>2014-08-19</fecha> <firmante>El Jefe de Servicio de Pruebas, Juan Español Español </firmante> </pieFirma> Ejemplo 2: <pieFirma> <lugar>Madrid</lugar> <fecha>2014-08-19</fecha> <firmante>El Subdirector General del Servicio de Pruebas, P.D. (Orden PRE/127/2013, de 3 de mayo), el Jefe del Servicio de Pruebas, Juan Español Español</firmante> </pieFirma>		[1..1]	complexType
2.4.2.8.2.1	lugar	Población en que tiene lugar la firma		[1..1]	string
2.4.2.8.2.2	fecha	Fecha de la firma en formato ISO 8601:2004 (aaaa-mm-dd).		[1..1]	string
2.4.2.8.2.3	firmante	Cargo y nombre y dos apellidos del firmante. En los casos de actuación administrativa automatizada puede consistir únicamente en la identificación del organismo o unidad firmante. En casos de alteración de la competencia deberán incluirse las referencias correspondientes. Este elemento debe estar informado.		[1..1]	string
2.4.2.9	contenidoCoof	Contenido del anuncio en lengua cooficial.		[0..1]	complexType
2.4.2.9.1	texto	Texto del anuncio. Incluirá de forma obligatoria un atributo content-type (tipo de dato string) con el valor "application/xml" El nodo texto estará formado por dos tipos de nodos que pueden repetirse tantas veces como sea necesario: párrafos (p) y tablas (table). El anuncio debe contener al menos un elemento párrafo. Si el texto cooficial lleva firma, debe ser incluido dentro de este elemento.		[1..1]	complexType
2.4.2.9.1.1	p	Párrafo de texto. Puede admitir un atributo class (tipo de dato string) para presentar la información. Este atributo puede tomar los siguientes valores: parrafo: Párrafo por defecto. titulo: Párrafo centrado con un tipo de letra mayor que el del párrafo por defecto. page-break: El elemento no tendrá contenido alguno. Fuerza un salto de página a partir de este elemento. Si no se indica el atributo, se le aplicará el atributo del párrafo por defecto. Ejemplos: Este es un párrafo normal Este es otro párrafo normal ANEXO		[1..*]	string
2.4.2.9.1.1.1	span	Dentro de un párrafo se podrán incluir elementos span con el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC, EXP o un nombre, para marcar un contenido a indexar si este no se ha incluido en el apartado metadatos/notificados. Por ejemplo: Se notifica a Juan Español Español con NIF 99999999R lo siguiente....			string
2.4.2.9.1.2	table	Tabla con información		[0..*]	complexType

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
2.4.2.9.1.2.1	caption	Título de la tabla		[0..1]	string
2.4.2.9.1.2.2	colgroup	Contiene información de las columnas de la tabla. Debe contener tantos elementos col como columnas tenga la tabla.		[0..1]	complexType
2.4.2.9.1.2.2.1	col	En él podrá especificarse si el contenido de la columna deberá ser indexado e incorporado al buscador añadiéndole el atributo class (tipo de dato string) con el valor index:NIF, index:NAF, index:CCC, index:EXP o index:NOMBRE, según sea el tipo del contenido un NIF, NAF, CCC o un nombre. Ejemplo: <colgroup> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col class="index:NIF"/> <col class="index:NOMBRE"/> <col /> <col /> <col /> </colgroup> En este ejemplo las columnas 1 y 3 de la tabla incluyen un NIF y las 2 y 4 un NOMBRE que deben incorporarse al buscador. Las columnas 5, 6 y 7 no se incorporarán al buscador.		[1..*]	complexType
2.4.2.9.1.2.3	thead	Cabecera de la tabla.		[0..1]	complexType
2.4.2.9.1.2.3.1	tr	Fila de la cabecera		[1..*]	complexType
2.4.2.9.1.2.3.1.1	th	Celda de la cabecera. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.9.1.2.4	tbody	Cuerpo de la tabla.		[1..1]	complexType
2.4.2.9.1.2.4.1	tr	Fila de la tabla		[1..*]	complexType
2.4.2.9.1.2.4.1.1	td	Celda de la tabla. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string
2.4.2.9.1.2.5	tfoot	Pie de la tabla. Normalmente no se usará.		[0..1]	complexType
2.4.2.9.1.2.5.1	tr	Fila del pie		[1..*]	complexType
2.4.2.9.1.2.5.1.1	th	Celda del pie. Admite los atributos rowspan (tipo de dato int) y colspan (tipo de dato int) para agrupamiento de celdas.		[1..*]	string"

ANEXO II

Formato XML para el envío de los documentos que deban insertarse en el Suplemento del Tablón Edictal Judicial Único

El contenido del envío se realizará en formato XML con la información estructurada de la siguiente forma:

```
<envio>
    <version>
    <remitente>
    <fechaPub>?
    <controlPub>
        <url>
        <email>
    </controlPub>
    <edictos>
        <edicto>+
            <emisor>
            <metadatos>?
                <id>?
                <sede>?
            </metadatos>
            <organo>
                <identificacion>
                <direccion>
                <localidad>
                <cp>
                <provincia>
                <telefono>?
                <email>?
            </organo>
            <contenido>+
                <procedimiento>
                    <tipo>
                    <numero>
                    <nig>
                </procedimiento>
                <resolucion>+
                    <tipo>
                    <fecha>
                    <objeto>+
                        <tipo>
                        <plazo>?<p></plazo>
```

```
                    </objeto>
                </resolucion>
                <destinatarios>?
                    <determinados>
                        <nombre>
                    </determinados>
                    <indeterminados>
                        <p>+
                    </indeterminados>
                </destinatarios>
                <observaciones>?
                    <p>+
                </observaciones>
            </contenido>
            <firma>
                <lugar>
                <fecha>
                <cargo>
                <firmante>
            </firma>
        </edicto>
    </edictos>
</envio>
```

\+ significa una o más ocurrencias.
? significa cero o una ocurrencia.
* significa cero o más ocurrencias.

A continuación se describen de forma pormenorizada cada uno de los elementos.

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
	envio	Nodo raíz del envío.		[1..1]	
1	version	Código que indica la versión utilizada. Existirá compatibilidad de versiones.	[1.0.0]	[1..1]	string
2	remitente	Código del órgano judicial remitente del edicto, que puede ser el mismo que el emisor o el de un servicio común que actúe como remitente de edictos emitidos por otros órganos judiciales.		[1..1]	string
3	fechaPub	Fecha de publicación solicitada en formato ISO 8601:2004 (aaaa-mm-dd).		[0..1]	string
4	controlPub	Información de control de publicación o devolución.		[1..1]	complexType
4.1	url	Dirección del servicio web a la que se informará de la fecha de publicación de los edictos o de su devolución.		[0..1]	anyUri
4.2	email	Dirección de correo electrónico a la que se informará la fecha de publicación de los edictos o de su devolución.		[1..1]	string
5	edictos	Lista de edictos que componen el envío.		[1..1]	complexType
5.1	edicto	Información relativa a un edicto.		[1..*]	complexType
5.1.1	emisor	Código del órgano judicial que emite el edicto *Nota: El emisor y el remitente será el mismo órgano judicial, salvo en el caso de los servicios comunes que actúen como remitentes de edictos emitidos por otros órganos judiciales.*		[1..1]	string
5.1.2	metadatos	Información que facilita la identificación de los edictos en los sistemas de información y su localización en la sede electrónica correspondiente.		[0..1]	complexType
5.1.2.1	id	Identificador único del edicto en los sistemas de información del órgano emisor o remitente. Este campo es opcional, aunque se recomienda que esté informado porque permite identificar posibles envíos de edictos duplicados.		[0..1]	string
5.1.2.2	sede	URL de la sede electrónica donde se encuentra disponible el edicto.		[0..1]	anyUri
5.1.3	organo	Datos del órgano emisor.		[1..1]	complexType
5.1.3.1	identificacion	Descripción textual (nombre) del órgano judicial.		[1..1]	string
5.1.3.2	direccion	Domicilio del órgano judicial.		[1..1]	string
5.1.3.3	localidad	Localidad del órgano judicial.		[1..1]	string
5.1.3.4	provincia	Código de provincia del órgano judicial. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.3.5	telefono	Teléfono del órgano judicial.		[0..1]	string
5.1.3.6	email	Dirección de correo electrónico del órgano judicial.		[0..*]	string
5.1.4	contenido	Contenido del edicto. Incluye el atributo idioma con el identificador del idioma en el que está escrito el edicto. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE. Pueden incluirse dos elementos de este tipo si el edicto se publica en lengua cooficial, además del castellano. En ese caso, ambos elementos tendrán los mismos valores, salvo para los campos «plazo» y «observaciones», que deberán ser redactados en la lengua correspondiente.		[1..2]	complexType
5.1.4.1	procedimiento	Datos del procedimiento.		[1..1]	complexType
5.1.4.1.1	tipo	Código del tipo de procedimiento. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.4.1.2	numero	Número de procedimiento, compuesto por el año (expresado con 4 dígitos) y el número secuencial dentro del año.		[1..1]	string
5.1.4.1.3	nig	Número de identificación general.		[0..1]	string
5.1.4.2	resolucion	Datos de la resolución.		[1..*]	complexType
5.1.4.2.1	tipo	Código del tipo de resolución. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.4.2.2	fecha	Fecha de la resolución en formato ISO 8601:2004 (aaaa-mm-dd).		[1..1]	string
5.1.4.2.3	objeto	Objeto del edicto.		[1..*]	complexType
5.1.4.2.3.1	tipo	Tipo de objeto, cuya tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.4.2.3.2	plazo	Indicaciones relativas al plazo para atender el tipo de objeto.		[0..1]	string
5.1.4.2.3.2.1	p	Párrafo de texto en el que se incluye las indicaciones relativas al plazo.		[1..1]	string

Esquema	Nombre	Descripción	Valores	Obl.	Tipo
5.1.4.3	destinatarios	Identificación de los destinatarios del edicto. Si existe este elemento, tiene que incluir o bien el elemento «determinados» o bien el elemento «indeterminados».		[0..*]	complexType
5.1.4.3.1	determinados	Identificación de los destinatarios determinados del edicto, si existen.		[1..1]	complexType
5.1.4.3.1.1	nombre	Nombre del destinatario. Incluye tres atributos para determinar la identificación: 1. tipoId: Tipo de identificador del destinatario, cuya tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE 2. id: Número de identificador 3. truncado: Permite que el órgano judicial indique si el número de identificador debe publicarse de forma íntegra o parcial.		[1..*]	string
5.1.4.3.2	indeterminados	Descripción de los destinatarios indeterminados del edicto.		[1..1]	complexType
5.1.4.3.2.1	p	Párrafo de texto con la descripción de los destinatarios indeterminados.		[1..*]	string
5.1.4.4	observaciones	Observaciones del emisor.		[0..1]	complexType
5.1.4.4.1	p	Párrafo de texto para que el órgano judicial incorpore la información complementaria que debe aparecer en el edicto.		[1..*]	string
5.1.5	firma	Pie de firma del anuncio.		[1..1]	complexType
5.1.5.1	lugar	Población en que tiene lugar la firma.		[1..1]	string
5.1.5.2	fecha	Fecha de la firma en formato ISO 8601:2004 (aaaa-mm-dd).		[1..1]	string
5.1.5.3	cargo	Código del cargo del firmante. La tabla de valores estará disponible en la sede electrónica de la Agencia Estatal BOE.		[1..1]	string
5.1.5.4	firmante	Nombre y dos apellidos del firmante.		[1..1]	string

§ 59

Orden PRE/1563/2006, de 19 de mayo, por la que se regula el procedimiento para la remisión telemática de las disposiciones y actos administrativos de los departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado»

Ministerio de la Presidencia
«BOE» núm. 123, de 24 de mayo de 2006
Última modificación: 24 de diciembre de 2018
Referencia: BOE-A-2006-9004

El procedimiento de publicación de disposiciones y actos de inserción obligatoria en el «Boletín Oficial del Estado» se encuentra regulado por el Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado. Aunque su artículo 15 prevé que los textos a publicar pueden presentarse en soportes técnicos distintos del papel, o transmitirse directamente de acuerdo con las garantías y especificaciones que se determinen, hasta ahora este procedimiento se ha configurado exclusivamente sobre el envío de disposiciones en soporte papel que en todo caso debe incorporar, como garantía de su autenticidad, firma autógrafa de la autoridad o funcionario autorizado al efecto.

Dadas las peculiaridades del procedimiento de publicación de disposiciones, la sustitución de documentos en soporte papel por documentos electrónicos ha de realizarse sin menoscabo de su principio rector que es el de velar, en todas y en cada una de sus fases de tramitación, por la correcta y fiel publicación de las disposiciones y actos administrativos que deben insertarse en el «Boletín Oficial del Estado», garantizando su autenticidad, la reserva sobre su contenido así como la competencia de la autoridad que ordena la inserción.

En el momento presente es posible automatizar con ese nivel de garantía el procedimiento de publicación de las disposiciones y actos administrativos de los departamentos ministeriales, agilizando las comunicaciones y los intercambios de documentación entre todos los sujetos participantes: los ministerios emisores de las disposiciones, la Dirección General del Secretariado del Gobierno, competente para la ordenación y control de su publicación y el organismo autónomo Boletín Oficial del Estado, al que corresponden las labores de impresión, distribución y venta del diario oficial.

El artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, establece, en su apartado 1, que las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias, y dispone, en su apartado 4, que los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características.

A su vez, el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado, desarrolla el artículo 45 de la citada Ley 30/1992 con la pretensión de delimitar, en el ámbito de la Administración General del Estado, las garantías, requisitos y supuestos de utilización de las técnicas electrónicas, informáticas y telemáticas.

La disposición adicional primera del Real Decreto 1229/2001, de 8 de noviembre, por el que se aprueba el Estatuto del organismo autónomo Boletín Oficial del Estado, habilita al titular del Ministerio de la Presidencia para establecer las garantías y especificaciones con arreglo a las cuales los originales destinados a la publicación en el «Boletín Oficial del Estado» podrán remitirse a través de medios electrónicos, informáticos y telemáticos.

En su virtud, previa aprobación del Ministro de Administraciones Públicas, dispongo:

Artículo 1. *Objeto.*

Esta orden tiene por objeto establecer el procedimiento de remisión telemática de las disposiciones y actos administrativos de los distintos departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado».

Artículo 2. *Ámbito de aplicación.*

La presente orden es de aplicación a todas aquellas disposiciones y actos administrativos de los departamentos ministeriales y sus organismos adscritos que no adopten la forma de real decreto y deban publicarse, de conformidad con lo previsto por el Real Decreto 1511/1986, de 6 de junio, de ordenación del diario oficial del Estado, en las secciones I, II y III del «Boletín Oficial del Estado».

Véase la Orden PRE/987/2008, de 8 de abril. Ref. BOE-A-2008-6370 y la Orden PCI/1377/2018, de 18 de diciembre. Ref. BOE-A-2018-17684, por la que se amplía el ámbito de aplicación.

Artículo 3. *Registro de firmas digitales.*

Sin perjuicio de lo previsto en el artículo 14 del Real Decreto 1511/1986, de 6 de junio, a fin de comprobar la autenticidad de los documentos electrónicos remitidos, la Dirección General del Secretariado del Gobierno llevará un registro de las firmas digitales de las autoridades y funcionarios facultados para firmar la inserción de los originales destinados a publicación.

A tal efecto, los titulares de firma de inserción deberán contar con un certificado de clase 2CA expedido por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

La Dirección General del Secretariado del Gobierno, competente para la ordenación y control de la publicación de las disposiciones y actos administrativos que deban insertarse en el «Boletín Oficial del Estado», comprobará la autenticidad e integridad de firmas electrónicas remitidas, así como el cumplimiento de los requisitos formales necesarios en cada caso.

Artículo 4. *Aprobación de la aplicación informática «Insértese digital».*

Los textos electrónicos de las disposiciones y actos administrativos de los departamentos ministeriales se remitirán a la Dirección General del Secretariado del Gobierno a través de la aplicación informática «Insértese digital» cuyas características figuran en el anexo de esta orden.

La aplicación informática «Insértese digital» es conforme con los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» publicados por Resolución de la Secretaría de Estado para la Administración Pública, de 26 de mayo de 2003.

Artículo 5. *Conservación de originales electrónicos.*

Sin perjuicio de la conservación de originales que corresponde realizar a los servicios de la Dirección General del Boletín Oficial del Estado, a efectos de lo previsto en el artículo 19 del Real Decreto 1511/1986, de 6 de junio, la Dirección General del Secretariado del Gobierno conservará, mediante un sistema de archivo que permita la consulta posterior y la prueba de su integridad, tanto el texto de los originales electrónicos remitidos como el de las firmas asociadas a ellos, así como el mecanismo de firma y la clave pública de la persona que ha firmado.

La conservación de originales electrónicos se realizará de conformidad con los requisitos recogidos en los «Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades» publicados por Resolución de la Secretaría de Estado para la Administración Pública, de 26 de mayo de 2003.

Artículo 6. *Remisión al organismo autónomo Boletín Oficial del Estado.*

La Dirección General del Secretariado del Gobierno remitirá al organismo autónomo Boletín Oficial del Estado los textos electrónicos de las disposiciones y actos administrativos firmados digitalmente. A tal efecto, este organismo llevará un registro de las firmas digitales de las autoridades y funcionarios de la Dirección General del Secretariado del Gobierno facultados para la remisión.

Artículo 7. *Instrucciones complementarias.*

La Subsecretaría de la Presidencia establecerá las instrucciones a las que deberán ajustarse los departamentos ministeriales para la remisión telemática de los originales electrónicos.

Artículo 8. *Entrada en vigor.*

Lo dispuesto en esta orden entrará en vigor el día 1 de junio de 2006.

ANEXO

Características de la aplicación informática «Insértese digital»

1. Objeto: la aplicación «Insértese digital» tiene por objeto posibilitar la remisión telemática a la Dirección General del Secretariado del Gobierno de las disposiciones y actos administrativos de los distintos departamentos ministeriales que deban publicarse en el «Boletín Oficial del Estado».

2. Funcionalidad: la aplicación «Insértese digital» ofrece las siguientes utilidades:

Firma electrónica de documentos empleando certificados de clase 2CA expedidos por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Transmisión telemática de los documentos firmados a la Dirección General del Secretariado del Gobierno del Ministerio de la Presidencia.

Verificación de la autenticidad e integridad de los documentos electrónicos recibidos y de sus firmas.

3. Órgano competente: Dirección General del Secretariado del Gobierno, conforme a lo previsto por el artículo 6.1 e) del Real Decreto 1418/2004, de 11 de junio, por el que se desarrolla la estructura orgánica básica del Ministerio de la Presidencia.

4. Usuarios de la aplicación:

Usuarios titulares de insértese, facultados para firmar la inserción de los documentos electrónicos destinados a publicación.

Usuarios tramitadores, facultados para remitir telemáticamente los documentos electrónicos firmados.

Los usuarios asumen con carácter exclusivo la responsabilidad de la custodia de los elementos de utilización personal necesarios para su autenticación en el acceso al sistema, el establecimiento de la conexión precisa y, en su caso, la utilización de firma electrónica.

5. Medios de acceso: el acceso a la aplicación se realizará a través de la intranet del Ministerio de la Presidencia, para lo cual deberá disponerse de una identificación de usuario y de la correspondiente clave de acceso.

§ 60

Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social

Ministerio de la Presidencia
«BOE» núm. 279, de 21 de noviembre de 2007
Última modificación: 19 de septiembre de 2018
Referencia: BOE-A-2007-19968

La Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, contiene una disposición final séptima, que encomienda al Gobierno fijar, en el plazo de dos años desde su entrada en vigor, unas condiciones básicas de accesibilidad y no discriminación para el acceso y utilización de las tecnologías, productos y servicios relacionados con la sociedad de la información y de cualquier medio de comunicación social.

En el mismo sentido, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en su disposición adicional quinta, obliga a las administraciones públicas a adoptar las medidas necesarias para que la información disponible en sus respectivas páginas de internet pueda ser accesible a personas mayores y con discapacidad de acuerdo con los criterios de accesibilidad al contenido generalmente reconocidos, antes del 31 de diciembre de 2005. La disposición adicional quinta establece, asimismo, que las administraciones públicas deben promover la adopción de normas de accesibilidad por parte de los prestadores de servicios y los fabricantes de equipos y de programas de ordenador, para facilitar el acceso de las personas mayores o con discapacidad a los contenidos digitales.

El Consejo de Ministros de 4 de noviembre de 2005 adoptó el Acuerdo por el que se aprueba el Plan 2006-2010 para el desarrollo de la sociedad de la información y de convergencia con Europa y entre comunidades autónomas y ciudades con estatuto de autonomía (Plan Avanza) que incluye un mandato dirigido al Ministerio de Trabajo y Asuntos Sociales, al Ministerio de Industria, Turismo y Comercio y al Ministerio de Administraciones Públicas para que elaboren un proyecto de real decreto por el que se regulen las condiciones de accesibilidad y no discriminación para el acceso y utilización de los servicios relacionados con la sociedad de la información, tomando en consideración, de manera particular, las recomendaciones europeas al respecto.

El presente real decreto se inspira en los principios establecidos en la Ley 51/2003, de 2 de diciembre, fundamentalmente, accesibilidad universal y diseño para todos.

Unos criterios de accesibilidad aplicables a las páginas de Internet son los que se recogen, a nivel internacional, en la Iniciativa de Accesibilidad a la Web (Web Accessibility

Initiative) del Consorcio Mundial de la Web (World Wide Web Consortium), que los ha determinado en forma de pautas comúnmente aceptadas en todas las esferas de internet, como las especificaciones de referencia cuando se trata de hacer que las páginas de Internet sean accesibles a las personas con discapacidad. En función de dichas pautas, la Iniciativa de Accesibilidad a la Web ha determinado tres niveles de accesibilidad: básico, medio y alto, que se conocen como niveles A, AA o doble A y AAA o triple A. Dichas pautas han sido incorporadas en España a través de la Norma UNE 139803:2004, que establece tres niveles de prioridades.

El presente real decreto especifica el grado de accesibilidad aplicable a las páginas de internet de las administraciones públicas, estableciendo como nivel mínimo obligatorio el cumplimiento de las prioridades 1 y 2 de la citada Norma UNE.

En la misma dirección, la Ley 10/2005, de 14 de junio, de medidas urgentes para el impulso de la televisión digital terrestre, de liberalización de la televisión por cable y de fomento del pluralismo, en su disposición adicional 2.ª, se refiere a la garantía de accesibilidad de la televisión digital terrestre para las personas con discapacidad, indicando que las administraciones competentes, previa audiencia a los representantes de los sectores afectados e interesados, adoptarán las medidas necesarias para garantizar desde el inicio la accesibilidad de las personas con discapacidad a los servicios de televisión digital terrestre, concretando que para conseguir este fin, las medidas que se adopten se atendrán a los principios de accesibilidad universal y diseño para todas las personas.

Asimismo, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, en su artículo 3, «Objetivos y principios», contempla la defensa de los intereses y la satisfacción de las necesidades de las personas con necesidades especiales, tales como las personas con discapacidad, y, en su artículo 22, establece, dentro del ámbito del servicio universal, que los usuarios finales con discapacidad deben tener acceso al servicio telefónico disponible al público desde una ubicación fija y a los demás elementos del servicio universal en condiciones equiparables a las que se ofrecen al resto de usuarios finales.

El reglamento de desarrollo de dicha ley, sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, concreta el ámbito del servicio universal, imponiendo obligaciones al operador designado en materia de accesibilidad, como las de garantizar la existencia de una oferta suficiente y tecnológicamente actualizada de terminales especiales adaptados a los diferentes tipos de discapacidades y realizar una difusión suficiente de la misma; la de poner a disposición de todos los usuarios, a través de internet, la guía telefónica en formato accesible; la de poner a disposición de los usuarios ciegos, o con grave discapacidad visual, una determinada franquicia en las llamadas al servicio de consulta telefónica sobre números de abonado, así como la de facilitar, de forma gratuita, las facturas y las condiciones de prestación del servicio, en sistema Braille o en letras grandes; la tarificación especial de las llamadas que se realicen desde cualquier punto del territorio nacional al Centro de Intermediación Telefónica para personas sordas o con discapacidad auditiva y/o de fonación del Ministerio de Trabajo y Asuntos Sociales; la obligación de elaborar planes de adaptación de las cabinas en la vía pública para facilitar su accesibilidad por los usuarios con discapacidad, en particular, por los usuarios ciegos, en silla de ruedas o de talla baja.

Finalmente, la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 4.c), establece el principio de accesibilidad a la información y a los servicios por medios electrónicos en los términos establecidos por la normativa vigente en esta materia, a través de sistemas que permitan obtenerlos de manera segura y comprensible, garantizando especialmente la accesibilidad universal y el diseño para todos los soportes, canales y entornos con objeto de que todas las personas puedan ejercer sus derechos en igualdad de condiciones, incorporando las características necesarias para garantizar la accesibilidad de aquellos colectivos que lo requieran.

El presente real decreto, en su disposición adicional primera, amplía las prestaciones que el operador designado ha de ofrecer, modificando el reglamento del servicio universal. En concreto, se incorpora la obligación de que la guía telefónica sea accesible a través de internet con las condiciones de accesibilidad previstas para las páginas web de las administraciones públicas; se amplían las obligaciones relativas a la adaptación de los

teléfonos públicos de pago, de forma que en los citados planes se contemplen expresamente las medidas para facilitar el acceso por usuarios ciegos. Además, dichos planes deberán contemplar la accesibilidad para personas con grave discapacidad visual, tanto de la información visual que se exhiba en el visor del terminal, como de la que figura en la propia cabina. Finalmente, se refuerza la obligación del operador designado en relación con la oferta de terminales fijos adaptados a los distintos tipos de discapacidad y se menciona expresamente la inclusión de soluciones para que las personas con discapacidad visual puedan acceder a los contenidos de las pantallas.

Por otra parte, en el Plan Nacional de Accesibilidad 2004-2012, adoptado por Acuerdo del Consejo de Ministros de 5 de julio de 2003, se pone de relieve que el uso que las personas con discapacidad hacen de las tecnologías, sistemas, productos y servicios relacionados con la comunicación, la información y la señalización es superior al de la media española.

La utilización de los nuevos recursos tecnológicos está muy a menudo vinculada a la calidad de vida, la normalización y la integración en la sociedad de las personas con discapacidad. Por esto, las barreras que se producen en este campo son de especial importancia y han de ser eliminadas de raíz. El presente real decreto se dicta con ese propósito.

El presente real decreto ha sido sometido a consulta de la XXXVI Conferencia Sectorial de Asuntos Sociales, del Consejo Nacional de la Discapacidad, de la Comisión del Mercado de las Telecomunicaciones, del Consejo Asesor de las Telecomunicaciones y para la Sociedad de la Información y del Consejo Superior de Administración Electrónica. Asimismo, ha participado en su elaboración mediante consultas, el tejido social de la discapacidad articulado en torno al Comité Español de Representantes de Personas con Discapacidad.

En su virtud, a propuesta conjunta de los Ministros de Industria, Turismo y Comercio, de Trabajo y Asuntos Sociales y de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de noviembre de 2007,

D I S P O N G O :

Artículo único. *Aprobación del Reglamento.*

Se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

Disposición adicional primera. *Modificación del Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.*

El Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, se modifica en los siguientes términos:

Uno. Se añade un segundo párrafo al artículo 30.2 en relación con la accesibilidad de la guía telefónica universal a través de internet:

> «El operador designado deberá ofrecer acceso a las guías telefónicas a través de Internet, en formato accesible para usuarios con discapacidad, en las condiciones y plazos de accesibilidad establecidos para las páginas de internet de las administraciones públicas, en el reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.»

Dos. El párrafo segundo del apartado 4 del artículo 32, queda redactado de la siguiente manera:

> «Para ello, el operador designado presentará, para su aprobación por el Ministerio de Industria, Turismo y Comercio, planes de adaptación de los teléfonos públicos de pago para facilitar su accesibilidad por los usuarios con discapacidad y, en particular, por los usuarios ciegos, en silla de ruedas o de talla baja. En relación

con los usuarios ciegos, los planes deberán contemplar la accesibilidad, tanto de la información dinámica facilitada por el visor de terminal, como de la estática a la que se refiere el apartado 3.f) de este artículo. Dichos planes se deberán presentar con un año de antelación a la finalización del que estuviera vigente o cuando el Ministerio de Industria, Turismo y Comercio lo demande por considerar superado el vigente.»

Tres. El párrafo primero del apartado 2 del artículo 33 queda redactado como sigue:

«A los efectos de lo dispuesto en el apartado anterior, el operador designado garantizará la existencia de una oferta suficiente y tecnológicamente actualizada de terminales especiales, adaptados a los diferentes tipos de discapacidades, tales como teléfonos de texto, videoteléfonos o teléfonos con amplificación para personas con discapacidad auditiva, o soluciones para que las personas con discapacidad visual puedan acceder a los contenidos de las pantallas de los terminales, y realizará una difusión suficiente de aquélla.»

Cuatro. El párrafo 2.º del apartado 2.a) del artículo 35, queda redactado del siguiente modo:

«2.º Usuarios ciegos o con grave discapacidad visual. Consistirá en la aplicación de una determinada franquicia en las llamadas al servicio de consulta telefónica sobre números de abonado, y en el establecimiento de las condiciones para la recepción gratuita de las facturas y de la publicidad e información suministrada a los demás abonados de telefonía fija sobre las condiciones de prestación de los servicios, en sistema Braille o en letras o caracteres ampliados, sin menoscabo de la oferta que de esta información se pueda realizar en otros sistemas o formatos alternativos.»

Disposición adicional segunda. *Apoyos complementarios.*

De acuerdo con lo ordenado por el artículo 10.2 c) de la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, se establecen los siguientes apoyos complementarios:

a) Las personas con discapacidad y sus familias podrán beneficiarse de las subvenciones y ayudas económicas que establezcan las administraciones públicas para la adquisición o contratación más ventajosa de elementos, bienes, productos y servicios de la sociedad de la información, en el ámbito de sus competencias.

b) Las personas mayores y con discapacidad tendrán la consideración de grupo de población prioritario en el acceso a las iniciativas, programas y acciones de infoinclusión y de extensión de la sociedad de la información que desarrollen las administraciones públicas. El Ministerio de Trabajo y Asuntos Sociales y el Ministerio de Industria, Turismo y Comercio, a través de los mecanismos adecuados y, en su caso, del Instituto Nacional de Tecnologías de la Comunicación, promoverán el acceso regular y normalizado de las personas con discapacidad a la sociedad de la información.

c) El Centro Estatal de Autonomía Personal y Ayudas Técnicas del Ministerio de Trabajo y Asuntos Sociales y el Ministerio de Industria Turismo y Comercio habilitarán una página de internet, accesible a las personas con discapacidad y mayores, que contendrá información global, completa y actualizada de todos los elementos, bienes, productos y servicios de la sociedad de la información, así como de las iniciativas, programas y acciones que se desarrollen en el ámbito de la sociedad de la información y los medios de comunicación social que tengan relevancia desde la perspectiva de las personas con discapacidad y mayores.

Disposición adicional tercera. *Consejo Nacional de la Discapacidad.*

El Consejo Nacional de la Discapacidad, con base en el informe anual o en las medidas o decisiones propuestas por la Oficina Permanente Especializada al Pleno, informará sobre el grado de cumplimiento de las obligaciones en materia de accesibilidad regulada en este real decreto, para ser tenido en cuenta por el departamento ministerial responsable.

Disposición transitoria única. *Plazos.*

1. Las obligaciones y medidas contenidas en este real decreto y el reglamento anexo serán exigibles desde el 4 de diciembre de 2009 para todos los productos y servicios nuevos, incluidas las campañas institucionales que se difundan en soporte audiovisual y desde el 4 de diciembre de 2013 para todos aquellos existentes que sean susceptibles de ajustes razonables.

2. Las páginas de internet de las administraciones públicas o con financiación pública deberán adaptarse a lo dispuesto en el artículo 5 de dicho reglamento, en los siguientes plazos:

a) Las páginas nuevas deberán ajustarse a la prioridad 1 de la Norma UNE 139803:2004 desde la entrada en vigor del real decreto.

b) Las páginas existentes deberán adaptarse a la prioridad 1 de la Norma UNE 139803:2004 en el plazo de 6 meses desde la entrada en vigor.

c) Todas las páginas, actualmente existentes o de nueva creación, deberán cumplir la prioridad 2 de la Norma UNE 139803:2004 a partir del 31 de diciembre de 2008. No obstante, este plazo de adaptación y la citada norma técnica de referencia podrán ser modificados a efectos de su actualización mediante orden ministerial conjunta, en los términos establecidos en la disposición final tercera de este real decreto.

3. Las obligaciones que la disposición adicional primera de este real decreto introduce en el reglamento aprobado por el Real Decreto 424/2005, de 15 de abril, deberán ser cumplidas a partir de la entrada en vigor del presente real decreto, a excepción de lo en ella previsto para la accesibilidad a la guía telefónica universal a través de Internet, a la que serán de aplicación los plazos establecidos en el apartado anterior.

Disposición final primera. *Financiación.*

Las medidas previstas en el presente real decreto, serán financiadas con cargo a los créditos ordinarios de los correspondientes departamentos y organismos públicos competentes.

Disposición final segunda. *Título competencial.*

1. Este real decreto se dicta al amparo de las reglas 1.ª y 21.ª del artículo 149.1 de la Constitución, que reservan al Estado, respectivamente, competencias para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales y en materia de telecomunicaciones.

2. Los artículos 5 y 8 del reglamento anexo al presente real decreto tienen el carácter de legislación básica sobre el régimen jurídico de las administraciones públicas, de conformidad con lo dispuesto en el artículo 149.1.18.ª de la Constitución.

Disposición final tercera. *Facultades de desarrollo.*

Se autoriza a los Ministros de Economía y Hacienda, de Trabajo y Asuntos Sociales, de Industria, Turismo y Comercio y de Administraciones Públicas, previa consulta al Consejo Nacional de la Discapacidad y al sector de operadores y empresas obligadas a cumplir las medidas del real decreto, a proponer al Ministro de la Presidencia la adopción mediante orden de cuantas disposiciones sean necesarias para la actualización de estándares determinados en el reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social o el reconocimiento de otros nuevos.

Disposición final cuarta. *Accesibilidad de páginas de internet.*

En al ámbito de la Administración General del Estado, la excepcionalidad prevista en el artículo 5.2 del Reglamento, se determinará por Orden de la Ministra de la Presidencia dictada a propuesta conjunta de los Ministros de Economía y Hacienda, de Trabajo y

Asuntos Sociales, de Industria, Turismo y Comercio y de la Ministra de Administraciones Públicas.

Disposición final quinta. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

REGLAMENTO SOBRE LAS CONDICIONES BÁSICAS PARA EL ACCESO DE LAS PERSONAS CON DISCAPACIDAD A LAS TECNOLOGÍAS, PRODUCTOS Y SERVICIOS RELACIONADOS CON LA SOCIEDAD DE LA INFORMACIÓN Y MEDIOS DE COMUNICACIÓN SOCIAL

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto del reglamento.*

El objeto de este reglamento es establecer los criterios y las condiciones que se consideran básicos para garantizar el acceso de las personas con discapacidad a las tecnologías, productos y servicios de la sociedad de la información y de cualquier medio de comunicación social, de acuerdo con los principios de igualdad de oportunidades, no discriminación y accesibilidad universal.

Artículo 2. *Ámbito de aplicación.*

Las administraciones públicas, los operadores de telecomunicaciones, los prestadores de servicios de la sociedad de la información y los titulares de medios de comunicación social que presten sus servicios bajo la jurisdicción española deberán cumplir las condiciones básicas de accesibilidad que se establecen en el presente reglamento.

CAPÍTULO II

Condiciones básicas de accesibilidad y no discriminación en materia de telecomunicaciones

Artículo 3. *Condiciones básicas de accesibilidad a los servicios de atención al cliente y al contenido de los contratos, facturas y demás información exigida.*

1. Los operadores deberán realizar los ajustes razonables que permitan el acceso por las personas con discapacidad al servicio de atención al cliente, referido en el artículo 104 del reglamento, aprobado por el Real Decreto 424/2005, de 15 de abril, en los plazos establecidos en la disposición final séptima de la Ley 51/2003, de 2 de diciembre.

2. Asimismo, los operadores deberán facilitar a los abonados con discapacidad visual que lo soliciten, en condiciones y formatos accesibles, los contratos, facturas, y demás información suministrada a todos los abonados en cumplimiento de lo dispuesto en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones y su normativa de desarrollo, en materia de derechos de los usuarios. Cuando la información o comunicación se realice a través de internet, será de aplicación lo dispuesto en este reglamento para las páginas de las administraciones públicas o con financiación pública.

Artículo 4. *Condiciones básicas de accesibilidad al servicio de telefonía móvil.*

1. Sin perjuicio de lo dispuesto en el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por el Real Decreto 424/2005, de 15 de abril, el Ministerio de Trabajo y Asuntos Sociales, a través del Centro Estatal de Autonomía Personal y Ayudas Técnicas, promoverá la existencia de una oferta suficiente y tecnológicamente actualizada de terminales de telefonía móvil especiales, adaptados a los diferentes tipos de

discapacidades. A estos efectos, se tendrán en consideración, entre otros, los siguientes elementos o facilidades:

a) Marcación vocal y gestión de las funciones principales del teléfono por voz.

b) Información, a través de una síntesis de voz, de las diferentes opciones disponibles en cada momento o de cualquier cambio que se produzca en la pantalla.

c) Generación de voz para facilitar la accesibilidad de los SMS.

d) Conectores para instalar equipos auxiliares tales como auriculares, amplificadores con bobina inductiva, pantallas externas, o teclados para enviar mensajes.

e) Pantallas de alto contraste, con caracteres grandes o ampliados y posibilidad de configuración por el usuario.

2. Cuando, de acuerdo con la Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicaciones y reconocimiento mutuo de su conformidad, la Comisión Europea decida la incorporación de requisitos adicionales en los equipos terminales de telefonía móvil, relativos a la compatibilidad de los mismos con las funcionalidades que faciliten su utilización por usuarios con discapacidad, su publicación en España se hará mediante resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, de acuerdo con lo dispuesto en el artículo 4 del Reglamento que establece el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones, aprobado por el Real Decreto 1890/2000, de 20 de noviembre.

CAPÍTULO III

Criterios y condiciones básicas de accesibilidad y no discriminación en materia de sociedad de la información

Artículo 5. *Criterios de accesibilidad aplicables a las páginas de internet de las administraciones públicas o con financiación pública.*

(Derogado).

Artículo 6. *Criterios de accesibilidad a otras páginas de internet.*

(Derogado).

Artículo 7. *Sistema de certificación de páginas de internet.*

(Derogado).

Artículo 8. *Condiciones básicas de accesibilidad a los equipos informáticos y a los programas de ordenador.*

1. Los equipos informáticos y los programas de ordenador -independientemente de que sea libre o esté sometido a derechos de patente o al pago de derechos-utilizados por las administraciones públicas, cuyo destino sea el uso por el público en general, deberán ser accesibles a las personas mayores y personas con discapacidad, de acuerdo con el principio rector de «Diseño para todos» y los requisitos concretos de accesibilidad exigidos, preferentemente en las normas técnicas nacionales que incorporen normas europeas, normas internacionales, otros sistemas de referencias técnicas elaborados por los organismos europeos de normalización o, en su defecto, normas nacionales (Normas UNE 139801:2003 y 139802:2003), y en los plazos establecidos en el apartado 1 de la disposición transitoria única del real decreto por el que se aprueba el presente reglamento.

2. Se deberán promover medidas de sensibilización y difusión para que los fabricantes de equipos informáticos y de programas de ordenador incorporen a sus productos y servicios, progresivamente y en la medida de lo posible, los criterios de accesibilidad y de «Diseño para todos», que faciliten el acceso de las personas mayores y personas con discapacidad a la sociedad de la información.

Artículo 9. *Condiciones básicas de accesibilidad en servicios y productos de confianza.*

Los servicios de confianza prestados y los productos para las personas usuarias finales utilizados en la prestación de estos servicios deberán ser accesibles para las personas mayores y personas con discapacidad. Excepcionalmente, esta obligación no será aplicable cuando el producto o servicio de confianza no disponga de una solución tecnológica que permita su accesibilidad.

CAPÍTULO IV

Condiciones básicas de accesibilidad y no discriminación en materia de medios de comunicación social

Artículo 10. *Condiciones básicas de accesibilidad a los contenidos de la televisión.*

1. Las personas con discapacidad tendrán acceso a los contenidos de los medios de comunicación audiovisual, con arreglo a las disponibilidades que permite el progreso técnico, los diseños universales y los ajustes razonables que, para atender las singularidades que presentan estas personas, sea preciso llevar a cabo.

2. Los contenidos audiovisuales de la televisión serán accesibles a las personas con discapacidad mediante la incorporación de la subtitulación, la audiodescripción y la interpretación en lengua de signos, en los términos establecidos específicamente en la legislación general audiovisual, que regulará, con carácter de norma básica, las condiciones de acceso y no discriminación en los contenidos de la televisión.

Artículo 11. *Condiciones básicas de accesibilidad a la televisión digital.*

1. Las administraciones públicas adoptarán las medidas necesarias para garantizar el acceso de las personas con discapacidad a los servicios de televisión digital, de acuerdo con los principios de accesibilidad universal y diseño para todas las personas.

2. Las administraciones públicas adoptarán las medidas necesarias para garantizar a las personas con discapacidad la existencia de una oferta suficiente de equipos receptores de televisión digital que permitan recibir sus contenidos, faciliten la navegación a través de los menús de configuración, las guías electrónicas de programación, los servicios interactivos y otros contenidos textuales, así como todas las prestaciones básicas que ofrecen los receptores de televisión digital, de acuerdo con los principios de accesibilidad universal y de diseño para todos.

Las herramientas de accesibilidad, que a tal efecto se utilicen, podrán integrar los siguientes elementos tecnológicos:

a) Conversión de texto a voz para favorecer la navegabilidad de los menús de configuración, las guías electrónicas de programación y los servicios interactivos y otros contenidos textuales.

b) Aplicaciones de reconocimiento de voz para efectuar operaciones de configuración, de solicitud de información de las guías electrónicas de programación o empleo de servicios interactivos u otros contenidos textuales.

c) Ergonomía en los receptores de televisión digital, así como en todos sus dispositivos asociados, y, muy especialmente, en el diseño de los mandos a distancia.

d) Aplicaciones de personalización para que, personas con discapacidad puedan configurar los receptores de televisión digital, y, muy particularmente, los parámetros de visualización: tamaño y color de la fuente de letras, color de fondo, contraste y otros.

e) Otras herramientas técnicas diseñadas para hacer accesibles los contenidos recibidos a través de la televisión digital a las personas con discapacidad, facilitando el manejo del receptor y permitiendo una recepción de la televisión digital sin barreras y adecuada al tipo y grado de discapacidad.

Las administraciones públicas, en la esfera de sus respectivas competencias, fomentarán la difusión pública de las medidas de accesibilidad a la televisión digital, coordinarán actuaciones y sinergias entre todos los agentes implicados, y desarrollarán planes de investigación, desarrollo e innovación (I+D+i), a fin de favorecer la implantación y la puesta en práctica de las tecnologías necesarias para que las personas con discapacidad

tengan pleno acceso a la televisión digital. Igualmente, las administraciones públicas implicadas, promoverán el desarrollo de políticas de normalización, códigos de buenas prácticas y herramientas que incorporen requisitos de accesibilidad.

Artículo 12. *Condiciones básicas de accesibilidad de la publicidad institucional en soporte audiovisual.*

1. De conformidad con lo dispuesto en la Ley 29/2005, de 29 de diciembre, de publicidad y comunicación institucional, aquellas campañas institucionales que se difundan en soporte audiovisual, preverán siempre en sus pliegos de cláusulas los procedimientos de acondicionamiento destinados a permitir que los mensajes contenidos sean accesibles para las personas con discapacidad y edad avanzada.

2. A los efectos de este artículo, la accesibilidad comprenderá la subtitulación en abierto de los mensajes hablados. Para la emisión en lengua de signos de los mensajes hablados (sistema de ventana menor en ángulo de la pantalla), la audiodescripción y la locución de todos los mensajes escritos que aparezcan, se estará a lo regulado por la Ley 27/2007, de 23 de octubre, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas. Todos estos procedimientos de acondicionamiento para permitir la accesibilidad se realizarán con arreglo a las normas técnicas establecidas para cada caso.

3. El presente artículo será de aplicación exclusiva en el ámbito de la Administración General del Estado y las demás entidades integrantes del sector público estatal.

§ 61

Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público

Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad
«BOE» núm. 227, de 19 de septiembre de 2018
Última modificación: 12 de agosto de 2019
Referencia: BOE-A-2018-12699

La Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público tiene como objeto, a fin de mejorar el funcionamiento del mercado interior, aproximar las disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a los requisitos de accesibilidad, entendiendo la accesibilidad como un conjunto de principios y técnicas que se deben respetar a la hora de diseñar, construir, mantener y actualizar los sitios web y las aplicaciones para dispositivos móviles.

La Directiva cubre todos los sitios web y aplicaciones móviles del sector público, desde los de la Administración estatal, Administraciones regionales y locales, Tribunales y órganos constitucionales a los de los servicios gestionados por éstas como Hospitales, Colegios, Universidades, Bibliotecas públicas, etc.

En este contexto, la Directiva exige que los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público se basen en requisitos comunes de accesibilidad establecidos a nivel europeo, poniendo fin a la fragmentación del mercado y a la diferenciación técnica hoy existente, evitando que los países apliquen diferentes versiones, niveles de cumplimiento o tengan diferencias técnicas a escala nacional, reduciendo la incertidumbre de los desarrolladores y fomentando la interoperabilidad. Aspectos todos, que deberían redundar en un aumento del potencial mercado interior de los productos y servicios relacionados con la accesibilidad de sitios web y aplicaciones para dispositivos móviles y por ende, contribuir al crecimiento económico y a la creación de empleo en la Unión Europea.

Para la consecución de este objetivo y asegurar que los ciudadanos se beneficien de un acceso más amplio a los servicios del sector público mediante sitios web y aplicaciones para dispositivos móviles cada vez más accesibles, la Directiva establece unos requisitos mínimos de accesibilidad obligatorios y adopta normas aplicables al diseño, construcción, mantenimiento y actualización de tales sitios web y aplicaciones para dispositivos móviles. A su vez, se impone la elaboración, actualización periódica y publicación de una declaración de accesibilidad sobre la conformidad de sus sitios web y aplicaciones para dispositivos móviles con los requisitos mínimos de accesibilidad que estén establecidos, facilitando la adaptación al estado de la técnica en cada momento. No obstante, la Directiva contempla excepciones al cumplimiento de estos requisitos cuando supongan una carga

desproporcionada para el organismo, sin que en ningún caso la falta de prioridad, tiempo o conocimientos puedan ser considerados como motivos legítimos para la excepción.

Por otro lado, para garantizar el cumplimiento de las previsiones establecidas en esta directiva se exige a cada Estado miembro la creación de un mecanismo de comunicación vinculado a un procedimiento de aplicación que permita, a cualquier persona usuaria de un sitio web o una aplicación para dispositivos móviles de un organismo del sector público, informar de la existencia de incumplimientos de los requisitos de accesibilidad, formular quejas y plantear sugerencias. Así como el establecimiento de un órgano, responsable del procedimiento de aplicación, que garantice que las comunicaciones y solicitudes recibidas se tratan de forma efectiva.

Asimismo, la Directiva (UE) 2016/2102, de 26 de octubre de 2016, impone a los Estados miembros la obligación de establecer un sistema de seguimiento y presentación de informes periódicos a la Comisión Europea, la adopción de medidas de promoción, formación y concienciación en materia de accesibilidad de todos los implicados y responsables jerárquicos y por último, invita a los Estados miembros a ampliar el ámbito de aplicación de sus normas a otros tipos de sitios web y de aplicaciones para dispositivos móviles.

Desde el punto de vista normativo la necesidad de regular unas condiciones básicas de accesibilidad para la utilización de servicios relacionados con la sociedad de la información se reconoce por primera vez en nuestro ordenamiento interno en la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad, que fijaba al Gobierno un plazo de dos años para su establecimiento. Los preceptos de dicha ley, actualmente derogada, se encuentran incluidos en el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el texto refundido de la Ley General de las personas con discapacidad y de su inclusión social.

Posteriormente, el 4 de diciembre de 2005, el Consejo de Ministros adoptó mediante Acuerdo el Plan 2006-2010 para el desarrollo de la sociedad de la información y de convergencia con Europa y entre comunidades autónomas y ciudades con Estatuto de autonomía (Plan Avanza), que incluía un mandato dirigido a los entonces Ministerio de Trabajo y Asuntos Sociales, al Ministerio de Industria, Turismo y Comercio y al Ministerio de Administraciones Públicas para que elaborasen un proyecto de real decreto que regulase dichas condiciones básicas. Fruto de este mandato es el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por el Real Decreto 1494/2007, de 12 de noviembre, que incluye en su capítulo III medidas específicas en materia de accesibilidad para las páginas de Internet de las Administraciones Públicas o entidades con financiación pública.

También existen otras normas que hacen referencia a los requisitos de accesibilidad de los sitios web de las Administraciones Públicas para las cuáles este nuevo real decreto asentará las bases. Algunas de ellas son la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, la Ley 27/2007, de 23 de octubre, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas, y la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014. Este real decreto viene a complementar al Real Decreto 1494/2007, de 12 de noviembre, y para ello deroga los artículos del reglamento que hacen referencia a la accesibilidad de las páginas de internet, los artículos 5, 6 y 7, y los desarrolla con mayor detalle. Por lo tanto, este Reglamento recoge los aspectos relativos a los requisitos mínimos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público, adoptando las medidas necesarias para cumplir con las disposiciones de la Directiva (UE) 2016/2102, de 26 de octubre de 2016, y, de este modo, seguir garantizando que la accesibilidad y no discriminación, en general y especialmente de las personas con discapacidad en sus relaciones con el sector público, sean reales y efectivas. A tal efecto, además de establecer

los requisitos mínimos que deben cumplirse e incorporar el resto de actuaciones previstas en la Directiva, este real decreto establece el sistema a través del cual las personas usuarias podrán comunicar al organismo del sector público cualquier posible incumplimiento por parte de su sitio web o de su aplicación para dispositivos móviles de los requisitos de accesibilidad establecidos y que también permita solicitar a las personas interesadas, previa solicitud razonable y legítima, la información sobre contenidos que están excluidos del ámbito de aplicación de este real decreto o exentos del cumplimiento de los requisitos de accesibilidad por imponer una carga desproporcionada.

La posibilidad de acudir al Defensor del Pueblo como propone la Directiva en su artículo 9, ya está recogida en la regulación española actual y se refleja en la Ley Orgánica 3/1981, de 6 de abril, del Defensor del Pueblo, que prevé la posibilidad de interponer quejas ante el Defensor del Pueblo para la defensa de los derechos del título I de la Constitución Española, y referidas al funcionamiento de la Administración, lo que incluye las actuaciones de todo el sector público en materia de accesibilidad con el nivel de obligaciones que imponga en cada momento la regulación vigente.

También existe la Oficina de Atención a la Discapacidad de acuerdo con lo previsto en el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013, de 29 de noviembre. Dicha Oficina es el órgano del Consejo Nacional de la Discapacidad, de carácter permanente y especializado, encargado de promover la igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y realiza las funciones de asesoramiento, análisis y estudio de las quejas, denuncias y consultas presentadas por las personas con discapacidad en los ámbitos de las telecomunicaciones y de la sociedad de la información, entre otras.

Por otro lado, este real decreto también incorpora, en una disposición adicional, los requisitos impuestos a las páginas de Internet de entidades, empresas y centros que prestan servicios públicos a través de una concesión pública, o alguna otra vía contractual con la Administración.

Asimismo, y también en una disposición adicional, se establecen los criterios de accesibilidad aplicables a los sitios web y aplicaciones para dispositivos móviles de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos, mediante la adecuación de su normativa específica a lo establecido en este real decreto, y siempre, de acuerdo con lo establecido en la misma.

Con respecto a su entrada en vigor, la Directiva da flexibilidad a los Estados Miembros exigiendo que como mínimo se apliquen todas las previsiones para sitios web nuevos antes del 23 de septiembre de 2019 y para todos los sitios web antes del 23 de septiembre de 2020. Considerando que en España se parte de una legislación existente en la que para sitos web ya se estaban exigiendo gran parte de estos requisitos, se ha diseñado la entrada en vigor de este real decreto dando continuidad a las previsiones del Real Decreto 1494/2007, de 12 de noviembre. De este modo, en el contexto español, se ha optado por una introducción escalonada en los mismos términos que la Directiva únicamente para los aspectos relacionados con la gestión de las quejas y reclamaciones y las aplicaciones móviles. También, atendiendo a las solicitudes recibidas desde el sector de las personas con discapacidad se han adelantado algunos de los plazos previstos en la Directiva. En cualquier caso, las previsiones de este real decreto se han adaptado temporalmente para hacer posible dar respuesta en tiempo y forma a la Comisión Europea con respecto al seguimiento y presentación de informes. El presente real decreto tiene carácter de legislación básica al amparo de lo dispuesto en el artículo 149.1.1.ª y 18.ª de la Constitución Española.

En la elaboración de este real decreto se han recabado los informes del Consejo Territorial de Servicios Sociales y del Sistema para la Autonomía y Atención a la Dependencia, del Consejo Estatal de las Personas Mayores, del Consejo Nacional de la Discapacidad, en el que tienen representación las organizaciones representativas de personas con discapacidad, del Consejo de Consumidores y Usuarios, del Consejo Estatal de Organizaciones no Gubernamentales de Acción Social, de la Comisión Sectorial de Administración Electrónica de la Conferencia Sectorial de Administración Pública, de la

Comisión de Estrategia TIC de la Administración General del Estado y del Comité Técnico Estatal de la Administración Judicial Electrónica.

El presente real decreto, que con arreglo al artículo 25 de la Ley 50/1997, de 27 de noviembre, del Gobierno, está incluido en el Plan Anual Normativo de 2018, asume el mandato de transposición de la Directiva (UE) 2016/2102, de 26 de octubre de 2016. La transposición se ha basado en los principios de la buena regulación previstos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. En particular, se ajusta al principio de necesidad y eficacia al cumplir la obligación de incorporación al derecho nacional con fidelidad al texto de la directiva; así como a los principios de proporcionalidad, al contener la regulación imprescindible para el fin que se persigue, transparencia, en la medida en que refuerza las garantías que lo rodean y favorece su cumplimiento, así como de seguridad jurídica, puesto que se realiza con el fin de mantener un marco normativo estable, predecible, integrado y claro.

En su virtud, a propuesta de la Ministra de Política Territorial y Función Pública, de la Ministra de Economía y Empresa y de la Ministra de Sanidad, Consumo y Bienestar Social, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 7 de septiembre de 2018,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto garantizar los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2.

2. A los efectos de este real decreto se entiende por accesibilidad el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los sitios web y las aplicaciones para dispositivos móviles para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

Artículo 2. *Ámbito subjetivo.*

1. Este real decreto se aplica al sector público que comprende:

a) La Administración General del Estado.

b) Las Administraciones de las comunidades autónomas.

c) Las entidades que integran la Administración Local.

d) El sector público institucional, en los términos establecidos en el artículo 2.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones públicas

e) Las asociaciones constituidas por las Administraciones, entes, organismos y entidades que integran el sector público.

2. Lo dispuesto en este real decreto también será de aplicación a la Administración de Justicia.

Artículo 3. *Ámbito objetivo de aplicación.*

1. Este real decreto se aplica tanto a los sitios web, independientemente del dispositivo empleado para acceder a ellos, como a las aplicaciones para dispositivos móviles de los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2.

2. El contenido accesible de los sitios web y de las aplicaciones para dispositivos móviles incluye la información tanto textual como no textual, los documentos y formularios que se

pueden descargar, los contenidos multimedia pregrabados de base temporal, las formas de interacción bidireccional, el tratamiento de formularios digitales y la cumplimentación de los procesos de identificación, autenticación, firma y pago con independencia de la plataforma tecnológica que se use para su puesta a disposición del público.

3. Están excluidos de este real decreto y se regularán por su normativa específica los contenidos multimedia en directo y pregrabado de base temporal de los sitios web y aplicaciones para dispositivos móviles de prestadores del servicio público de radiodifusión y sus filiales, así como los de otros organismos o sus filiales que cumplan un mandato de servicio público de radiodifusión.

4. Asimismo, quedan excluidos del ámbito de aplicación del presente real decreto los siguientes contenidos:

a) Formatos de archivo de ofimática publicados antes de la entrada en vigor de este real decreto, salvo que los mismos sean necesarios para tareas administrativas activas relativas a las funciones realizadas por los sujetos obligados por este real decreto.

b) Contenido multimedia pregrabado de base temporal publicado antes de la entrada en vigor de este real decreto.

c) Contenido multimedia en directo de base temporal salvo lo dispuesto en otra legislación específica que obligue al respecto.

d) Servicios de mapas y cartografía en línea, siempre y cuando la información esencial se proporcione de manera accesible digitalmente en el caso de mapas destinados a fines de navegación.

e) Contenidos de terceros que no estén financiados ni desarrollados por el sujeto obligado ni estén bajo su control.

f) Reproducciones de bienes de colecciones del patrimonio que no puedan hacerse plenamente accesibles por alguna de las siguientes causas:

1.° Incompatibilidad de los requisitos de accesibilidad con la conservación del bien de que se trate o con la autenticidad de la reproducción.

2.° Indisponibilidad de soluciones automatizadas y rentables que permitan extraer el texto de manuscritos u otros bienes de colecciones del patrimonio y transformarlos en contenidos compatibles con los requisitos de accesibilidad.

g) Contenidos de extranet e intranet entendidos como sitios web accesibles únicamente para un grupo restringido de personas y no para el público en general, publicados antes del 23 de septiembre de 2019, hasta que dichos sitios web sean objeto de una revisión sustancial.

h) Contenidos de sitios web y aplicaciones para dispositivos móviles que tengan la condición de archivos o herramientas de archivo por contener únicamente contenidos no necesarios para el desarrollo de cualesquiera tareas administrativas activas, siempre que no hayan sido actualizados ni editados con posterioridad a la entrada en vigor de este real decreto.

Artículo 4. *Definiciones.*

A efectos del presente real decreto se entiende por:

a) Sitio web: Es un conjunto de archivos electrónicos y páginas web referentes a un tema en particular bajo un nombre de dominio específico a los que se accede utilizando un navegador web.

b) Aplicaciones para dispositivos móviles: Son las aplicaciones informáticas diseñadas y desarrolladas para ser usadas por el público en general en dispositivos móviles, entre los que se incluyen los teléfonos inteligentes y las tabletas. No incluyen el programa «software» que controla dichos dispositivos (sistemas operativos para dispositivos móviles) ni el equipo informático.

c) Archivo ofimático: Son los documentos que no están destinados, en principio, a ser utilizados en la web, pero están incluidos en sitios web, pudiendo estar realizados, entre otros, en formato estándar Portable Document Format (PDF), o habiendo sido confeccionados mediante procesadores de texto, hojas de cálculo o aplicaciones para la realización de presentaciones.

d) Bienes de colecciones de patrimonio: Son los bienes de propiedad pública o privada que presentan un interés histórico, arqueológico, estético, científico o técnico y que forman parte de colecciones conservadas por instituciones culturales como bibliotecas, archivos y museos.

e) Contenido de los sitios web y de las aplicaciones para dispositivos móviles: Es la información tanto textual como no textual, los documentos y formularios que se pueden descargar, así como las formas de interacción bidireccional, como el tratamiento de formularios digitales y la cumplimentación de los procesos de identificación, autenticación, firma y pago.

f) Contenido multimedia de base temporal: Son los ficheros multimedia que pueden ser de los siguientes tipos: Solo audio, solo vídeo, audio y vídeo, o cualquiera de los anteriores combinado con interacción.

g) Contenidos multimedia pregrabados: Son los contenidos multimedia de base temporal emitidos en directo que se mantienen en línea o se vuelven a emitir tras su transmisión en directo, inmediatamente después de la fecha de la emisión inicial o la nueva emisión.

h) Datos de las mediciones: Son los resultados cuantificados de la actividad de seguimiento llevada a cabo a fin de comprobar la conformidad de los sitios web y las aplicaciones para dispositivos móviles con los requisitos de accesibilidad exigidos. Incluyen tanto la información cuantitativa sobre las muestras de sitios web y aplicaciones para dispositivos móviles comprobadas como la información cuantitativa sobre el nivel de accesibilidad.

i) Norma: Son las especificaciones técnicas adoptadas por un organismo de normalización reconocido, de aplicación repetida o continua, cuya observancia no es obligatoria.

j) Norma europea: Es una norma adoptada por una organización europea de normalización.

k) Norma armonizada: Es una norma europea adoptada a raíz de una petición de la Comisión Europea para la aplicación de la legislación de armonización de la Unión Europea.

l) Perceptibilidad: Es el principio de la accesibilidad que exige que la información y los componentes de la interfaz de usuario se presenten a las personas usuarias de manera que pueda percibirlos.

m) Operabilidad: Es el principio de la accesibilidad que exige que los componentes y la navegación de la interfaz de usuario se puedan utilizar por cualquier persona usuaria.

n) Comprensibilidad: Es el principio de la accesibilidad que exige que la información y el funcionamiento de la interfaz de usuario sean comprensibles por cualquier persona usuaria.

ñ) Robustez: Es el principio de la accesibilidad que exige que los contenidos sean suficientemente sólidos para poder ser interpretados de forma fiable por una gran variedad de agentes de usuario, incluidas las tecnologías de asistencia.

Artículo 5. *Requisitos para la accesibilidad de los sitios web y aplicaciones para dispositivos móviles.*

1. Los sitios web y aplicaciones para dispositivos móviles de las entidades obligadas incluidas en el ámbito de aplicación del presente real decreto deberán ser accesibles para sus personas usuarias y, en particular, para las personas mayores y personas con discapacidad, de modo que sus contenidos sean perceptibles, operables, comprensibles y robustos teniendo en cuenta las normas del artículo 6.

2. La accesibilidad se tendrá presente de forma integral en el proceso de diseño, gestión, mantenimiento y actualización de contenidos de los sitios web y las aplicaciones para dispositivos móviles.

3. Las entidades obligadas adoptarán, siempre que sea posible, medidas para aumentar la accesibilidad de sus sitios web y aplicaciones para dispositivos móviles respecto del nivel mínimo de accesibilidad que deba cumplirse en cada momento.

Artículo 6. *Presunción de conformidad con los requisitos de accesibilidad.*

1. Se presumirá que el contenido de los sitios web y aplicaciones para dispositivos móviles que cumpla las normas armonizadas o partes de éstas cuyas referencias hayan sido publicadas en el «Diario Oficial de la Unión Europea» es conforme a los requisitos de

accesibilidad establecidos en el artículo 5 que estén cubiertos por dichas normas o partes de ellas.

2. En caso de que no se hayan publicado las referencias de las normas armonizadas a que se refiere el apartado 1, se presumirá que el contenido de las aplicaciones para dispositivos móviles que cumpla las especificaciones técnicas o partes de éstas, que la Comisión haya adoptado mediante los correspondientes actos de ejecución, es conforme a los requisitos de accesibilidad establecidos en el artículo 5 que estén cubiertos por dichas especificaciones técnicas o partes de ellas.

3. En caso de que no se hayan publicado las referencias de las normas armonizadas a que se refiere el apartado 1, se presumirá que el contenido de los sitios web que cumpla los requisitos pertinentes de la norma EN 301 549 V1.1.2 (2015-04) o partes de estos, es conforme a los requisitos de accesibilidad establecidos en el artículo 5 que estén cubiertos por dichos requisitos o partes de ellos.

En caso de que no se hayan publicado las referencias de las normas armonizadas a que se refiere el apartado 1, y en ausencia de las especificaciones técnicas a que se refiere el apartado 2, se presumirá que el contenido de aplicaciones para dispositivos móviles que cumpla los requisitos pertinentes de la norma EN 301 549 V1.1.2 (2015-04) o partes de estos, es conforme a los requisitos de accesibilidad establecidos en el artículo 5 que estén cubiertos por dichos requisitos o partes de ellos.

4. Se aplicarán directamente las actualizaciones de referencias a la norma EN 301 549 V1.1.2 (2015-04) que la Comisión adopte mediante actos delegados para hacer referencia a una versión más reciente de dicha norma o a una norma europea que la sustituya.

5. El órgano encargado de realizar el seguimiento y presentación de informes ante la Comisión Europea mantendrá disponible en su sitio web la referencia concreta a las normas armonizadas, normas y especificaciones técnicas que sean de aplicación en cada momento.

Artículo 7. *Carga desproporcionada.*

1. Con carácter excepcional, en atención a la carga desproporcionada que el cumplimiento de los requisitos de accesibilidad pueda suponer para la entidad obligada, se podrá exceptuar el cumplimiento de los requisitos de accesibilidad recogidos en el presente real decreto.

La excepción al cumplimiento de los requisitos de accesibilidad deberá ser motivada y se limitará al contenido concreto y a lo estrictamente necesario para reducir la carga. No obstante, la entidad deberá hacer estos contenidos lo más accesibles posible y cumplir todos los requisitos de accesibilidad en el resto de contenidos.

2. Se considera carga desproporcionada aquella que impone a la entidad obligada una carga financiera y organizativa excesiva, o que compromete su capacidad para cumplir su cometido o para publicar la información necesaria y pertinente para sus tareas y servicios, teniendo en cuenta al mismo tiempo el posible beneficio o perjuicio para los ciudadanos, en particular para las personas con discapacidad y personas mayores.

3. No se consideran motivos que permitan apreciar la excepción de la carga desproporcionada la falta de prioridad, de tiempo o de conocimientos. Asimismo, tampoco es posible justificar la necesidad de adquirir o desarrollar sistemas informáticos, para la gestión de contenidos de sitios web, y aplicaciones para dispositivos móviles que no sean accesibles.

4. A fin de evaluar en qué medida el cumplimiento de los requisitos de accesibilidad previstos en este real decreto impone una carga desproporcionada, las entidades obligadas deberán tener en cuenta como mínimo las siguientes circunstancias:

a) El tamaño, los recursos y la naturaleza del sujeto concreto obligado.

b) Los costes y beneficios estimados para el mismo, en relación con los beneficios estimados para las personas con discapacidad y las personas mayores, teniendo en cuenta la frecuencia y la duración del uso del sitio web o aplicación para dispositivos móviles en especial.

5. La entidad obligada concreta que desee acogerse a la excepción contemplada en el apartado 1 de este artículo deberá llevar a cabo una evaluación inicial de la medida en que el cumplimiento de los requisitos de accesibilidad previstos en este real decreto impone una

carga desproporcionada debiéndolo hacer constar por escrito mediante el correspondiente informe. Dicha evaluación deberá revisarse al menos una vez al año para contemplar los posibles cambios organizacionales o técnicos.

6. En todo caso, en la declaración de accesibilidad para el sitio web concreto o la aplicación para dispositivos móviles concreta, después de realizar la correspondiente evaluación, se hará constar las partes de los requisitos de accesibilidad que no puede cumplir y, en su caso, se ofrecerá alternativas accesibles según los términos definidos en el artículo 15.

Artículo 8. *Promoción, concienciación y formación.*

1. Los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2 adoptarán medidas de sensibilización y divulgación para incrementar la concienciación dentro de las Administraciones Públicas y en la sociedad en general sobre los requisitos de accesibilidad y la universalidad de sus beneficios, así como sobre todas las medidas puestas en práctica con este real decreto, especialmente la posibilidad y medios para reclamar en caso de incumplimiento de las previsiones establecidas.

2. En particular, las entidades obligadas velarán por la concienciación en materia de accesibilidad de todo el personal a su servicio y específicamente de aquellos órganos o Unidades con competencias en el desarrollo de los sitios web y las aplicaciones para dispositivos móviles del sector público, así como de los encargados de la edición y generación de sus contenidos.

3. Las entidades obligadas fomentarán y facilitarán programas de formación internos que garanticen conocimientos actualizados sobre las condiciones de accesibilidad en la creación, gestión y actualización de los contenidos de los sitios web y aplicaciones para dispositivos móviles. Para ello:

a) Los correspondientes institutos y organismos competentes en materia de formación en la Función Pública incluirán en sus planes de formación actividades en relación con la accesibilidad de los sitios web y sus contenidos y de las aplicaciones para dispositivos móviles.

b) Las entidades obligadas establecerán, como complemento de los anteriores, programas de formación específicos en la materia para el personal a su servicio, especialmente, para quienes pertenezcan a órganos o unidades con competencias en el desarrollo de los sitios web y las aplicaciones para dispositivos móviles así como, para las personas encargadas de la edición y generación de contenidos.

4. Los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2 promoverán medidas de sensibilización, divulgación, educación y formación en el terreno de la accesibilidad, con objeto de lograr que los titulares de otros sitios web o aplicaciones móviles distintas de aquéllas a las que se refiere este real decreto, incorporen progresivamente y en la medida de lo posible los criterios de accesibilidad, particularmente aquéllas cuyo contenido se refiera a bienes y servicios a disposición del público.

5. Respecto de las webs y dispositivos móviles, los organismos del sector público y otros obligados incluidos en el ámbito de aplicación del artículo 2 observarán los mandatos sobre promoción de la accesibilidad universal contenidos en las disposiciones normativas específicas en materia de contratación pública y harán uso de las facultades y posibilidades que esta legislación ofrece a los órganos contratantes, para ampliar y elevar los niveles de accesibilidad digital en la adquisición de bienes, productos y servicios.

Artículo 9. *Participación de las personas interesadas.*

Las Administraciones Públicas determinarán los mecanismos de participación de las personas interesadas y de las personas usuarias en el seguimiento de las políticas de accesibilidad de los sitios web y las aplicaciones para dispositivos móviles, teniendo en cuenta especialmente a las organizaciones representativas de personas con discapacidad y personas mayores, y sus familias.

CAPÍTULO II

Comunicaciones, quejas y reclamaciones

Artículo 10. *Mecanismos de comunicación.*

1. Las entidades obligadas deberán ofrecer a las personas usuarias un mecanismo de comunicación que permita a cualquier persona presentar sugerencias y quejas, así como informar sobre cualquier posible incumplimiento por parte de su sitio web o de su aplicación para dispositivos móviles de los requisitos de accesibilidad y solicitar la información excluida.

2. Se distinguen dos modalidades en función de la naturaleza de la comunicación y de los efectos y tratamiento que ésta vaya a tener:

a) Comunicaciones sobre requisitos de accesibilidad. Permite a cualquier persona física y jurídica informar sobre cualquier posible incumplimiento por parte del sitio web o de la aplicación para dispositivos móviles de los requisitos de accesibilidad establecidos. También permite transmitir otras dificultades de acceso al contenido o formular cualquier otra consulta o sugerencia de mejora relativa a la accesibilidad del sitio web o aplicación para dispositivos móviles.

b) Solicitudes de información accesible y quejas. Permite a cualquier persona física o jurídica formular quejas relativas al cumplimiento de los requisitos de este real decreto y solicitar la información relativa a contenidos que están excluidos del ámbito de aplicación de este real decreto según lo establecido por el artículo 3, apartado 4, o exentos del cumplimiento de los requisitos de accesibilidad por imponer una carga desproporcionada.

Artículo 11. *Comunicaciones sobre requisitos de accesibilidad.*

Las comunicaciones sobre requisitos de accesibilidad podrán presentarse mediante medios electrónicos habilitando una dirección de correo electrónico específica o un formulario que permita la presentación telemática. Adicionalmente, se habilitará al menos uno de los siguientes canales complementarios al electrónico: Un teléfono o una oficina física de atención.

Artículo 12. *Solicitudes de información accesible y quejas.*

1. Las solicitudes de información accesible y quejas serán presentadas y registradas conforme a los requisitos establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

2. En el caso de las solicitudes de información accesible, la persona interesada deberá concretar, con toda claridad, los hechos, razones y petición que permitan constatar que se trata de una solicitud razonable y legítima.

3. Recibidas las solicitudes de información accesible y quejas, la entidad obligada deberá responder a la persona interesada en el plazo de veinte días hábiles.

4. El transcurso de dicho plazo se podrá suspender en el caso de que deba requerirse a la persona interesada para que, en un plazo de diez días hábiles, formule las aclaraciones necesarias para la correcta tramitación de la solicitud de información accesible o queja. Transcurrido dicho plazo sin que la persona interesada haya realizado las aclaraciones oportunas, se continuará con su tramitación.

5. La respuesta deberá incluir la siguiente información:

a) La Unidad que emite la respuesta.

b) La decisión que se ha adoptado.

c) En su caso, la información accesible solicitada.

d) En su caso, el plazo estimativo y la Unidad responsable de llevar a cabo las medidas para corregir un posible incumplimiento, si las mismas no se pueden adoptar de inmediato.

e) La Unidad ante la cual se puede reclamar y el procedimiento por el cual se puede hacer la reclamación.

6. Transcurrido el plazo máximo para resolver sin que se haya notificado la respuesta se entenderá que la solicitud de información accesible no ha sido aceptada o que la queja no ha sido considerada.

Téngase en cuenta que se declara que los apartados 1, 3, 4 y 6 invaden las competencias autonómicas y carecen de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

Artículo 13. *Procedimiento de reclamación.*

1. Si una vez realizada una solicitud de información accesible o queja, ésta hubiera sido desestimada, no se estuviera de acuerdo con la decisión adoptada, o la respuesta no cumpliera los requisitos contemplados en el artículo 12.5, la persona interesada podrá iniciar una reclamación para conocer y oponerse a los motivos de la desestimación, instar la adopción de las medidas oportunas en el caso de no estar de acuerdo con la decisión adoptada, o exponer las razones por las que se considera que la respuesta no cumple con los requisitos exigidos.

Igualmente se podrá iniciar una reclamación en el caso de que haya trascurrido el plazo **de veinte días hábiles** sin haber obtenido respuesta.

2. Dicha reclamación deberá ser presentada y registrada conforme a los requisitos establecidos en la Ley 39/2015, de 1 de octubre.

La reclamación deberá dirigirse a la Unidad responsable de accesibilidad de ese ámbito competencial, o si la respuesta se hubiera realizado desde la propia Unidad responsable de accesibilidad, al superior jerárquico de ésta.

3. Las entidades obligadas deberán incluir en la declaración de accesibilidad la Unidad a la cual elevar las reclamaciones junto con el enlace al sistema de registro en el que se deberá realizar dicha reclamación.

4. Recibida la reclamación, la Unidad responsable de atenderla deberá responder a la persona interesada en el plazo máximo de dos meses.

5. El transcurso de dicho plazo se podrá suspender en el caso de que deba requerirse a la persona interesada para que, en un plazo de diez días hábiles, formule las aclaraciones necesarias para la correcta tramitación de la reclamación. Transcurrido dicho plazo sin que la persona interesada haya realizado las aclaraciones oportunas, se continuará con la tramitación de la reclamación.

6. Transcurrido el plazo máximo para resolver la reclamación sin que se haya notificado la resolución de la misma, se entenderá que la reclamación ha sido desestimada.

Téngase en cuenta que se declara que el inciso destacado del apartado 1 y los apartados 2 a 6 invaden las competencias autonómicas y carecen de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

Artículo 14. *Recursos.*

Contra la resolución de la reclamación regulada en los anteriores artículos se podrán interponer los recursos administrativos que procedan, de conformidad con lo dispuesto en el artículo 112 de la Ley 39/2015, de 1 de octubre de 2015.

CAPÍTULO III

Control, revisión, seguimiento y presentación de informes

Artículo 15. *Declaración de accesibilidad.*

1. Las entidades responsables de las webs y aplicaciones para móviles proporcionarán una declaración de accesibilidad detallada, exhaustiva y clara sobre la conformidad de sus respectivos sitios web y aplicaciones para dispositivos móviles con lo dispuesto en este real

decreto. Dicha declaración será actualizada periódicamente, como mínimo una vez al año, o cada vez que se realice una revisión de accesibilidad conforme a lo especificado en el artículo 17.

Esta declaración de accesibilidad se proporcionará en un formato accesible haciendo uso de las instrucciones y del modelo de declaración de accesibilidad que se establezca conforme a lo dispuesto en el apartado 3.

En el caso de los sitios web, la declaración se publicará en el sitio web correspondiente estando disponible su acceso desde todas las páginas del sitio web con un enlace denominado «Accesibilidad» o su equivalente en el idioma en el que se encuentre disponible la página.

En el caso de las aplicaciones para dispositivos móviles, la declaración estará disponible en el sitio web de la entidad obligada que haya desarrollado la aplicación concreta para dispositivos móviles junto con el enlace para su descarga o bien se facilitará junto con otra información disponible al descargar la aplicación de las plataformas de distribución de aplicaciones.

2. La declaración de accesibilidad comprenderá, como mínimo, la siguiente información:

a) Una explicación sobre aquellas partes del contenido que no sean accesibles y las razones de dicha inaccesibilidad, así como, en su caso, las alternativas accesibles que se ofrezcan.

b) Un enlace y descripción del mecanismo de comunicación en los términos que se establecen en los artículos 10, 11 y 12 del presente real decreto.

c) Un enlace al procedimiento de reclamación regulado en el artículo 13 al que cualquier persona interesada pueda recurrir en caso de que la respuesta a la comunicación o a la solicitud sea insatisfactoria.

3. Mediante Orden de la Ministra de Política Territorial y Función Pública se aprobarán instrucciones específicas para la generación y puesta a disposición de las declaraciones de accesibilidad **de aplicación en todo el territorio nacional** de acuerdo con los requisitos especificados en el modelo europeo.

> Téngase en cuenta que se declara inconstitucional y nulo el inciso destacado del apartado 3 y que el texto restante de dicho apartado invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

Artículo 16. *Unidad responsable de accesibilidad.*

1. Cada entidad obligada determinará la Unidad responsable de garantizar el cumplimiento de los requisitos de accesibilidad de los sitios web y aplicaciones para dispositivos móviles dentro de su ámbito competencial.

En la Administración General del Estado se designarán las Unidades responsables de accesibilidad en el ámbito de las Subsecretarías de cada Departamento considerando todos los posibles organismos públicos y entidades de derecho público dependientes de ese Departamento.

En las comunidades autónomas se designará la Unidad responsable de accesibilidad para todo el ámbito autonómico.

En las entidades locales y demás organismos obligados se designará, conforme a sus características organizativas propias, la Unidad responsable de accesibilidad de su ámbito.

2. La Unidad responsable de accesibilidad definirá el modelo de funcionamiento dentro de su ámbito competencial actuando directamente sobre todo el ámbito o con un posible esquema de responsables de accesibilidad delegados en los diferentes organismos o entidades dependientes.

Téngase en cuenta que se declara que el apartado 2 invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

3. La Unidad responsable de accesibilidad tendrá las siguientes funciones:

a) Coordinar y velar por el funcionamiento efectivo de los mecanismos de comunicación establecidos en el capítulo II ayudando a la definición, emitiendo directrices y promoviendo la existencia de los medios y procedimientos para garantizar una adecuada gestión y atención de cuantas consultas, sugerencias, comunicaciones, quejas y solicitudes de información accesible se reciban en cada uno de los órganos, organismos o entidades bajo su competencia.

b) Atender y dar respuesta a las reclamaciones que, en aplicación de lo dispuesto en el artículo 13 le sean dirigidas.

c) Revisar las evaluaciones realizadas para acogerse a la excepción del cumplimiento de los requisitos de accesibilidad por imponer éstos una carga desproporcionada regulada en el artículo 7.

d) Coordinar las revisiones periódicas de accesibilidad establecidas en el artículo 17, con la colaboración, en su caso, de las Unidades de tecnologías de la información y comunicaciones.

e) Coordinar y fomentar las actividades de promoción, concienciación y formación establecidas en el artículo 8.

f) Realizar los informes que se determinen para garantizar el cumplimiento de las previsiones establecidas en el artículo 19.

g) Actuar como punto de contacto con el organismo encargado de realizar el seguimiento y presentación de informes y colaborar con las tareas que tiene asignadas

h) Cualesquiera otras, que en garantía de la accesibilidad de los sitios web y aplicaciones para dispositivos móviles le puedan ser atribuidas.

4. Se deberá notificar al órgano encargado de realizar el seguimiento y presentación de informes al que se refiere el artículo 18 las designaciones, modificaciones o bajas de las correspondientes Unidades responsables de accesibilidad.

Artículo 17. *Revisión de la accesibilidad.*

1. Las entidades obligadas por el presente real decreto realizarán revisiones del cumplimiento de los requisitos de accesibilidad establecidos tanto en la fase de diseño de los sitios web y aplicaciones para dispositivos móviles como antes de su puesta en funcionamiento.

2. Una vez puesto en funcionamiento un sitio web o aplicación para dispositivos móviles, las entidades obligadas realizarán revisiones periódicas del cumplimiento de los requisitos de accesibilidad con el fin de garantizar el mantenimiento de su cumplimiento a lo largo del tiempo. Especialmente, se deberá tener en cuenta el caso de los contenidos añadidos o modificados durante el ciclo de vida de los sitios web así como las actualizaciones tecnológicas de estos últimos y de las aplicaciones para dispositivos móviles.

3. Las revisiones de accesibilidad deberán abarcar todos los requisitos exigidos y tendrán en consideración tanto aspectos de revisión automática como aspectos de revisión manual experta. El resultado de éstas deberá quedar recogido en un informe de revisión de la accesibilidad.

4. Mediante Orden de la Ministra de Política Territorial y Función Pública se podrá aprobar un modelo y condiciones específicas para realizar estas revisiones de accesibilidad que podrán ampliar lo establecido en la metodología europea para el seguimiento de la conformidad. En cualquier caso, estas revisiones deberán respetar las condiciones mínimas exigidas para las revisiones en profundidad de un sitio web o aplicación móvil que establezca la metodología europea.

Téngase en cuenta que se declara que la primera frase del apartado 4 invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

5. Las entidades obligadas podrán certificar el cumplimiento de los requisitos de este real decreto en sus sitios web y aplicaciones para dispositivos móviles por una entidad de certificación cuya competencia técnica haya sido reconocida formalmente por la Entidad Nacional de Acreditación (ENAC) o por otro organismo nacional de acuerdo al Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

6. En cualquier caso, la primera revisión de accesibilidad deberá haberse realizado en el caso de los sitios web antes de dos años desde la entrada en vigor de este real decreto, y, en el caso de las aplicaciones móviles, antes de tres años desde la entrada en vigor de este real decreto.

Artículo 18. *Seguimiento y presentación de informes.*

1. El órgano encargado de realizar el seguimiento y presentación de informes ante la Comisión Europea es el Ministerio de Política Territorial y Función Pública.

2. Este órgano podrá comprobar periódicamente el estado de situación con respecto a la conformidad de los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público con los requisitos de accesibilidad, basándose en la metodología para el seguimiento de la conformidad prevista en el artículo 8.2 de la Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público según sea determinado por la Comisión Europea en los correspondientes actos de ejecución.

Este órgano también podrá realizar verificaciones sobre muestras aleatorias con respecto a la exactitud de los informes de revisión de la accesibilidad definidos en el artículo 17.

3. Este órgano presentará a la Comisión Europea, a más tardar el 23 de diciembre de 2021 y posteriormente cada tres años, un informe sobre el resultado del seguimiento que se hará público en formato accesible.

4. Dicho informe deberá ajustarse a lo que se determine en los actos de ejecución que adoptará la Comisión Europea para la presentación de informes de Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016. En cualquier caso deberá incluir:

a) Los datos de las mediciones.

b) Información sobre el uso del procedimiento de reclamación establecido en el artículo 13.

c) Información sobre los elementos enumerados en el apartado 5 cuando hayan sido objeto de cambios significativos respecto del informe anterior.

5. El primer informe comprenderá también:

a) Una descripción de los mecanismos creados en España para consultar a las personas interesadas sobre la accesibilidad de los sitios web y las aplicaciones para dispositivos móviles;

b) procedimientos para hacer pública cualquier evolución de las políticas de accesibilidad relacionada con los sitios web y las aplicaciones para dispositivos móviles;

c) experiencias y conclusiones extraídas de la aplicación de las normas sobre conformidad con los requisitos de accesibilidad establecidos;

d) información sobre actividades de formación y concienciación.

Artículo 19. *Coordinación para el seguimiento y presentación de informes.*

1. Cada Unidad responsable de accesibilidad preparará tres informes anuales sobre su ámbito de actuación concreto que tendrá disponibles antes del 1 de octubre de cada año a partir del año 2020:

a) Informe sobre la atención de quejas y reclamaciones. Dicho informe incluirá las medidas puestas en práctica para atender las cuestiones planteadas en el artículo 16.3.a) junto a un estudio de las comunicaciones, consultas, sugerencias, solicitudes de información accesible y quejas formuladas a través del mismo. También incluirá un estudio de las reclamaciones atendidas y revisiones realizadas según el artículo 16.3.b) y c).

b) Informe de seguimiento sobre el cumplimiento de los requisitos de accesibilidad dentro de su ámbito competencial incluyendo las medidas puestas en marcha para atender las acciones contempladas en el artículo 16.3.d) y los resultados derivados de ellas. Asimismo, se incluirán todos los informes de revisión de la accesibilidad realizados según lo previsto en el artículo 17.

c) Informe de seguimiento sobre la promoción, concienciación y formación dentro de su ámbito competencial incluyendo las medidas puestas en marcha para atender las acciones contempladas en el artículo 16.3.e) y los resultados derivados de ellas.

2. Para facilitar las tareas del Ministerio de Política Territorial y Función Pública colaborarán con éste: La Red de Contactos de Accesibilidad Digital de las Administraciones Públicas del artículo 20, todas las Unidades responsables de accesibilidad y todos los actores implicados en las diferentes actividades de revisión de la accesibilidad, procedimiento de reclamación, promoción y concienciación, formación, y coordinación previstas en el presente real decreto.

Para ello deberán suministrar la información específica en tales áreas con los modelos, condicionantes y procedimientos que establezca el Ministerio de Política Territorial y Función Pública.

3. **Para la definición de los modelos, condicionantes y procedimientos que permitan conocer regularmente e informar** sobre estas materias, **el Ministerio de Política Territorial y Función Pública** podrá contar con la participación de:

a) La Red de Contactos de Accesibilidad Digital de las Administraciones Públicas.

b) Los órganos de coordinación en materia de tecnologías de la información de la Administración General del Estado previstos en el Real Decreto 806/2014, de 19 de septiembre.

c) La Comisión Sectorial de Administración Electrónica establecida en la disposición adicional novena de la Ley 40/2015, de 2 de octubre, de Régimen Jurídico del Sector Público.

d) El Comité Técnico Estatal De La Administración Judicial Electrónica establecido en el artículo 44 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Téngase en cuenta que se declara que el inciso destacado del apartado 3 invade las competencias autonómicas y carecen de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

Artículo 20. *Red de Contactos de Accesibilidad Digital de las Administraciones Públicas.*

1. Se crea la Red de Contactos de Accesibilidad Digital de las Administraciones Públicas con funciones de asistencia al Ministerio de Política Territorial y Función Pública regulado en el artículo 18, que tendrá la consideración de grupo de trabajo de los previstos en el artículo 22.3 de la Ley 40/2015, de 1 de octubre.

2. La Red de Contactos de Accesibilidad Digital de las Administraciones Públicas estará integrada por:

a) Las personas titulares de las Unidades responsables de accesibilidad de la Administración General del Estado.

b) Las personas titulares de las Unidades responsables de accesibilidad de las comunidades autónomas.

c) Al menos un punto de contacto provincial que agrupará a las entidades locales de esa provincia y que podrá estar provisto por la correspondiente Diputación Provincial, Comunidad Autónoma, Consorcio o Federación de municipios considerando sus características territoriales concretas y de acuerdo con la normativa específica de régimen local.

d) Una persona designada al respecto por parte de la Conferencia de Rectores para las Universidades españolas que agrupará a las Universidades.

e) Una persona designada al respecto por parte del Comité Técnico Estatal de la Administración Judicial Electrónica que agrupará a las entidades del ámbito judicial.

f) Las personas titulares de las Unidades responsables de accesibilidad de los demás entes obligados que no estén cubiertos por los anteriormente indicados.

g) Las asociaciones comprendidas en el artículo 2.1.e participarán a través de uno de los miembros anteriormente indicados considerando el tipo de la entidad con participación mayoritaria en la asociación.

3. Los personas integrantes de esta red de contactos actuarán como difusoras y agregadoras de la información disponible de todas las entidades a las que representen o agrupen.

4. Las designaciones, modificaciones o bajas de las personas integrantes de esta red deberán ser notificadas al Ministerio de Política Territorial y Función Pública.

Disposición adicional primera. *Criterios de accesibilidad aplicables a los sitios web y aplicaciones para dispositivos móviles con financiación pública.*

Las Administraciones Públicas exigirán que se apliquen los criterios de accesibilidad de los artículos 5 y 6 del presente real decreto a:

a) Los sitios web y aplicaciones para dispositivos móviles que reciban financiación pública para su diseño o mantenimiento.

b) Los sitios web y aplicaciones para dispositivos móviles, vinculados a la prestación de servicios públicos, de entidades y empresas que se encarguen, ya sea por vía concesional o a través de otra vía contractual, de gestionar servicios públicos, en especial, los que tengan carácter educativo, sanitario, cultural, deportivo y de servicios sociales.

c) Los sitios web y aplicaciones para dispositivos móviles de los centros privados educativos, de formación y universitarios sostenidos, total o parcialmente, con fondos públicos.

Disposición adicional segunda. *Criterios de accesibilidad aplicables a los sitios web y aplicaciones para dispositivos móviles de los órganos constitucionales del Estado y de los órganos legislativos y de control autonómicos.*

Los criterios de accesibilidad recogidos en el presente real decreto, serán de aplicación a los sitios web y aplicaciones para dispositivos móviles de los órganos competentes del Congreso de los Diputados, del Senado, del Consejo de Estado, del Consejo Económico y Social, del Consejo General del Poder Judicial, del Tribunal Constitucional, del Tribunal de Cuentas, del Defensor del Pueblo, del Banco de España, **de las Asambleas legislativas de las comunidades autónomas**, así como a las instituciones autonómicas que realicen funciones análogas, en relación con sus actividades sujetas a Derecho Administrativo y con sujeción a su normativa específica.

Téngase en cuenta que se declara inconstitucional y nulo el inciso destacado, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

El titular de la Unidad responsable de accesibilidad de cada uno de estos órganos podrá formar parte, si así lo decide la institución concernida, de la Red de Contactos de Accesibilidad Digital de las Administraciones Públicas.

Disposición adicional tercera. *Lenguas de signos españolas y medios de apoyo a la comunicación oral.*

Respecto de las lenguas de signos españolas y los medios de apoyo a la comunicación oral, los sitios web y las aplicaciones móviles tendrán en cuenta lo que disponga específicamente la Ley 27/2007, de 23 de octubre, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas y sus normas de desarrollo.

Disposición adicional cuarta. *No incremento de gastos de personal y Unidades responsables de accesibilidad en la Administración General del Estado.*

Conforme a lo establecido en la disposición adicional trigésima novena de la Ley 6/2018, de 3 de julio, de Presupuestos Generales del Estado para el año 2018, las medidas incluidas en esta norma no podrán suponer en el ámbito de la Administración General del Estado incremento de dotaciones, ni de retribuciones, ni de otros gastos de personal.

Las funciones que corresponda desarrollar a las Unidades responsables de accesibilidad serán asignadas a Unidades ya existentes.

Disposición transitoria única. *Modelo de declaración.*

En tanto no se publique el modelo de declaración al que se refiere el artículo 15, se aplicará por defecto el modelo de declaración de accesibilidad que la Comisión Europea establezca mediante los correspondientes actos de ejecución previstos en la Directiva (UE) 2016/2102, de 26 de octubre de 2016.

Téngase en cuenta que se declara que esta disposición invade las competencias autonómicas y carece de carácter de legislación básica, por Sentencia del TC 100/2019, de 18 de julio. Ref. BOE-A-2019-11912

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente real decreto y, específicamente, los artículos 5, 6 y 7 del Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.

Disposición final primera. *Modificación del Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por el Real Decreto 1494/2007, de 12 de noviembre.*

El artículo 9 del Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social, aprobado por el Real Decreto 1494/2007, de 12 de noviembre, quedará redactado en la forma siguiente:

> **«Artículo 9.** *Condiciones básicas de accesibilidad en servicios y productos de confianza.*
>
> Los servicios de confianza prestados y los productos para las personas usuarias finales utilizados en la prestación de estos servicios deberán ser accesibles para las

personas mayores y personas con discapacidad. Excepcionalmente, esta obligación no será aplicable cuando el producto o servicio de confianza no disponga de una solución tecnológica que permita su accesibilidad.»

Disposición final segunda. *Título competencial.*

La presente norma se dicta al amparo de lo dispuesto en el artículo 149.1.1.ª y 18.ª de la Constitución, que atribuye al Estado las competencias para «la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales» y, para regular «las bases del régimen jurídico de las Administraciones Públicas y el procedimiento administrativo común», respectivamente.

Disposición final tercera. *Incorporación de derecho comunitario.*

Mediante el presente real decreto se incorpora al ordenamiento jurídico la Directiva (UE) 2016/2102, del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público.

Disposición final cuarta. *Desarrollo normativo.*

Se faculta a los titulares del Ministerio de Política Territorial y Función Pública y del Ministerio de Economía y Empresa, en el ámbito de sus respectivas competencias, para dictar las disposiciones adicionales necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, así como para acordar las medidas precisas para garantizar su ejecución e implantación efectiva, sin perjuicio de las competencias propias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final quinta. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado» con las siguientes excepciones:

Para los sitios web, las disposiciones previstas en los artículos 10.2.b), 12 y 13 serán de aplicación al año de la entrada en vigor de este real decreto, y a los dos años para los sitios web ya publicados.

Todas las disposiciones relativas a aplicaciones para dispositivos móviles serán de aplicación desde el 23 de junio de 2021.

§ 62

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

Jefatura del Estado
«BOE» núm. 294, de 6 de diciembre de 2018
Última modificación: 9 de mayo de 2023
Referencia: BOE-A-2018-16673

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley orgánica.

PREÁMBULO

I

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus

orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

II

En los últimos años de la pasada década se intensificaron los impulsos tendentes a lograr una regulación más uniforme del derecho fundamental a la protección de datos en el marco de una sociedad cada vez más globalizada. Así, se fueron adoptando en distintas instancias internacionales propuestas para la reforma del marco vigente. Y en este marco la Comisión lanzó el 4 de noviembre de 2010 su Comunicación titulada «Un enfoque global de la protección de los datos personales en la Unión Europea», que constituye el germen de la posterior reforma del marco de la Unión Europea. Al propio tiempo, el Tribunal de Justicia de la Unión ha venido adoptando a lo largo de los últimos años una jurisprudencia que resulta fundamental en su interpretación.

El último hito en esta evolución tuvo lugar con la adopción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

III

El Reglamento general de protección de datos pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. La transposición de la directiva por los Estados miembros se ha plasmado en un mosaico normativo con perfiles irregulares en el conjunto de la Unión Europea lo que, en último extremo, ha conducido a que existan diferencias apreciables en la protección de los derechos de los ciudadanos.

Asimismo, se atiende a nuevas circunstancias, principalmente el aumento de los flujos transfronterizos de datos personales como consecuencia del funcionamiento del mercado interior, los retos planteados por la rápida evolución tecnológica y la globalización, que ha hecho que los datos personales sean el recurso fundamental de la sociedad de la información. El carácter central de la información personal tiene aspectos positivos, porque permite nuevos y mejores servicios, productos o hallazgos científicos. Pero tiene también

riesgos, pues las informaciones sobre los individuos se multiplican exponencialmente, son más accesibles, por más actores, y cada vez son más fáciles de procesar mientras que es más difícil el control de su destino y uso.

El Reglamento general de protección de datos supone la revisión de las bases legales del modelo europeo de protección de datos más allá de una mera actualización de la vigente normativa. Procede a reforzar la seguridad jurídica y transparencia a la vez que permite que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios. Así, el Reglamento general de protección de datos contiene un buen número de habilitaciones, cuando no imposiciones, a los Estados miembros, a fin de regular determinadas materias, permitiendo incluso en su considerando 8, y a diferencia de lo que constituye principio general del Derecho de la Unión Europea que, cuando sus normas deban ser especificadas, interpretadas o, excepcionalmente, restringidas por el Derecho de los Estados miembros, estos tengan la posibilidad de incorporar al derecho nacional previsiones contenidas específicamente en el reglamento, en la medida en que sea necesario por razones de coherencia y comprensión.

En este punto hay que subrayar que no se excluye toda intervención del Derecho interno en los ámbitos concernidos por los reglamentos europeos. Al contrario, tal intervención puede ser procedente, incluso necesaria, tanto para la depuración del ordenamiento nacional como para el desarrollo o complemento del reglamento de que se trate. Así, el principio de seguridad jurídica, en su vertiente positiva, obliga a los Estados miembros a integrar el ordenamiento europeo en el interno de una manera lo suficientemente clara y pública como para permitir su pleno conocimiento tanto por los operadores jurídicos como por los propios ciudadanos, en tanto que, en su vertiente negativa, implica la obligación para tales Estados de eliminar situaciones de incertidumbre derivadas de la existencia de normas en el Derecho nacional incompatibles con el europeo. De esta segunda vertiente se colige la consiguiente obligación de depurar el ordenamiento jurídico. En definitiva, el principio de seguridad jurídica obliga a que la normativa interna que resulte incompatible con el Derecho de la Unión Europea quede definitivamente eliminada «mediante disposiciones internas de carácter obligatorio que tengan el mismo valor jurídico que las disposiciones internas que deban modificarse» (Sentencias del Tribunal de Justicia de 23 de febrero de 2006, asunto Comisión vs. España; de 13 de julio de 2000, asunto Comisión vs. Francia; y de 15 de octubre de 1986, asunto Comisión vs. Italia). Por último, los reglamentos, pese a su característica de aplicabilidad directa, en la práctica pueden exigir otras normas internas complementarias para hacer plenamente efectiva su aplicación. En este sentido, más que de incorporación cabría hablar de «desarrollo» o complemento del Derecho de la Unión Europea.

La adaptación al Reglamento general de protección de datos, que será aplicable a partir del 25 de mayo de 2018, según establece su artículo 99, requiere, en suma, la elaboración de una nueva ley orgánica que sustituya a la actual. En esta labor se han preservado los principios de buena regulación, al tratarse de una norma necesaria para la adaptación del ordenamiento español a la citada disposición europea y proporcional a este objetivo, siendo su razón última procurar seguridad jurídica.

IV

Internet, por otra parte, se ha convertido en una realidad omnipresente tanto en nuestra vida personal como colectiva. Una gran parte de nuestra actividad profesional, económica y privada se desarrolla en la Red y adquiere una importancia fundamental tanto para la comunicación humana como para el desarrollo de nuestra vida en sociedad. Ya en los años noventa, y conscientes del impacto que iba a producir Internet en nuestras vidas, los pioneros de la Red propusieron elaborar una Declaración de los Derechos del Hombre y del Ciudadano en Internet.

Hoy identificamos con bastante claridad los riesgos y oportunidades que el mundo de las redes ofrece a la ciudadanía. Corresponde a los poderes públicos impulsar políticas que hagan efectivos los derechos de la ciudadanía en Internet promoviendo la igualdad de los ciudadanos y de los grupos en los que se integran para hacer posible el pleno ejercicio de los derechos fundamentales en la realidad digital. La transformación digital de nuestra

sociedad es ya una realidad en nuestro desarrollo presente y futuro tanto a nivel social como económico. En este contexto, países de nuestro entorno ya han aprobado normativa que refuerza los derechos digitales de la ciudadanía.

Los constituyentes de 1978 ya intuyeron el enorme impacto que los avances tecnológicos provocarían en nuestra sociedad y, en particular, en el disfrute de los derechos fundamentales. Una deseable futura reforma de la Constitución debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales. Pero, en tanto no se acometa este reto, el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española y que, en algunos casos, ya han sido perfilados por la jurisprudencia ordinaria, constitucional y europea.

V

Esta ley orgánica consta de noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales.

El Título I, relativo a las disposiciones generales, comienza regulando el objeto de la ley orgánica, que es, conforme a lo que se ha indicado, doble. Así, en primer lugar, se pretende lograr la adaptación del ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, Reglamento general de protección de datos, y completar sus disposiciones. A su vez, establece que el derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica. Las comunidades autónomas ostentan competencias de desarrollo normativo y ejecución del derecho fundamental a la protección de datos personales en su ámbito de actividad y a las autoridades autonómicas de protección de datos que se creen les corresponde contribuir a garantizar este derecho fundamental de la ciudadanía. En segundo lugar, es también objeto de la ley garantizar los derechos digitales de la ciudadanía, al amparo de lo dispuesto en el artículo 18.4 de la Constitución.

Destaca la novedosa regulación de los datos referidos a las personas fallecidas, pues, tras excluir del ámbito de aplicación de la ley su tratamiento, se permite que las personas vinculadas al fallecido por razones familiares o de hecho o sus herederos puedan solicitar el acceso a los mismos, así como su rectificación o supresión, en su caso con sujeción a las instrucciones del fallecido. También excluye del ámbito de aplicación los tratamientos que se rijan por disposiciones específicas, en referencia, entre otras, a la normativa que transponga la citada Directiva (UE) 2016/680, previéndose en la disposición transitoria cuarta la aplicación a estos tratamientos de la Ley Orgánica 15/1999, de 13 de diciembre, hasta que se apruebe la citada normativa.

En el Título II, «Principios de protección de datos», se establece que a efectos del Reglamento (UE) 2016/679 no serán imputables al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos obtenidos directamente del afectado, cuando hubiera recibido los datos de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad, o cuando el responsable los obtuviese del mediador o intermediario cuando las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establezcan la posibilidad de intervención de un intermediario o mediador o cuando los datos hubiesen sido obtenidos de un registro público. También se recoge expresamente el deber de confidencialidad, el tratamiento de datos amparado por la ley, las categorías especiales de datos y el tratamiento de datos de naturaleza penal, se alude específicamente al consentimiento, que ha de proceder de una declaración o de una clara acción afirmativa del afectado, excluyendo lo que se conocía como «consentimiento tácito», se indica que el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que se otorga para todas ellas, y se mantiene en catorce años la edad a partir de la cual el menor puede prestar su consentimiento.

Se regulan asimismo las posibles habilitaciones legales para el tratamiento fundadas en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal, Este es el caso, por ejemplo, de las bases de datos reguladas por ley y gestionadas por autoridades públicas que responden a objetivos específicos de control de riesgos y solvencia, supervisión e inspección del tipo de la Central de Información de Riesgos del Banco de España regulada por la Ley 44/2002, de 22 de noviembre, de Medidas de Reforma del Sistema Financiero, o de los datos, documentos e informaciones de carácter reservado que obren en poder de la Dirección General de Seguros y Fondos de Pensiones de conformidad con lo previsto en la Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

Se podrán igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras, cuando ello derive del ejercicio de potestades públicas o del cumplimiento de una obligación legal y solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el reglamento europeo, cuando derive de una competencia atribuida por la ley. Y se mantiene la prohibición de consentir tratamientos con la finalidad principal de almacenar información identificativa de determinadas categorías de datos especialmente protegidos, lo que no impide que los mismos puedan ser objeto de tratamiento en los demás supuestos previstos en el Reglamento (UE) 2016/679. Así, por ejemplo, la prestación del consentimiento no dará cobertura a la creación de «listas negras» de sindicalistas, si bien los datos de afiliación sindical podrán ser tratados por el empresario para hacer posible el ejercicio de los derechos de los trabajadores al amparo del artículo 9.2.b) del Reglamento (UE) 2016/679 o por los propios sindicatos en los términos del artículo 9.2.d) de la misma norma europea.

También en relación con el tratamiento de categorías especiales de datos, el artículo 9.2 consagra el principio de reserva de ley para su habilitación en los supuestos previstos en el Reglamento (UE) 2016/679. Dicha previsión no sólo alcanza a las disposiciones que pudieran adoptarse en el futuro, sino que permite dejar a salvo las distintas habilitaciones legales actualmente existentes, tal y como se indica específicamente, respecto de la legislación sanitaria y aseguradora, en la disposición adicional decimoséptima. El Reglamento general de protección de datos no afecta a dichas habilitaciones, que siguen plenamente vigentes, permitiendo incluso llevar a cabo una interpretación extensiva de las mismas, como sucede, en particular, en cuanto al alcance del consentimiento del afectado o el uso de sus datos sin consentimiento en el ámbito de la investigación biomédica. A tal efecto, el apartado 2 de la Disposición adicional decimoséptima introduce una serie de previsiones encaminadas a garantizar el adecuado desarrollo de la investigación en materia de salud, y en particular la biomédica, ponderando los indudables beneficios que la misma aporta a la sociedad con las debidas garantías del derecho fundamental a la protección de datos.

El Título III, dedicado a los derechos de las personas, adapta al Derecho español el principio de transparencia en el tratamiento del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada «información por capas» ya generalmente aceptada en ámbitos como el de la videovigilancia o la instalación de dispositivos de almacenamiento masivo de datos (tales como las «cookies»), facilitando al afectado la información básica, si bien, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Se hace uso en este Título de la habilitación permitida por el considerando 8 del Reglamento (UE) 2016/679 para complementar su régimen, garantizando la adecuada estructura sistemática del texto. A continuación, la ley orgánica contempla los derechos de acceso, rectificación, supresión, oposición, derecho a la limitación del tratamiento y derecho a la portabilidad.

En el Título IV se recogen «Disposiciones aplicables a tratamientos concretos», incorporando una serie de supuestos que en ningún caso debe considerarse exhaustiva de

todos los tratamientos lícitos. Dentro de ellos cabe apreciar, en primer lugar, aquellos respecto de los que el legislador establece una presunción «iuris tantum» de prevalencia del interés legítimo del responsable cuando se lleven a cabo con una serie de requisitos, lo que no excluye la licitud de este tipo de tratamientos cuando no se cumplen estrictamente las condiciones previstas en el texto, si bien en este caso el responsable deberá llevar a cabo la ponderación legalmente exigible, al no presumirse la prevalencia de su interés legítimo. Junto a estos supuestos se recogen otros, tales como la videovigilancia, los ficheros de exclusión publicitaria o los sistemas de denuncias internas en que la licitud del tratamiento proviene de la existencia de un interés público, en los términos establecidos en el artículo 6.1.e) del Reglamento (UE) 2016/679. Finalmente, se hace referencia en este Título a la licitud de otros tratamientos regulados en el Capítulo IX del reglamento, como los relacionados con la función estadística o con fines de archivo de interés general. En todo caso, el hecho de que el legislador se refiera a la licitud de los tratamientos no enerva la obligación de los responsables de adoptar todas las medidas de responsabilidad activa establecidas en el Capítulo IV del reglamento europeo y en el Título V de esta ley orgánica.

El Título V se refiere al responsable y al encargado del tratamiento. Es preciso tener en cuenta que la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos personales para, a partir de dicha valoración, adoptar las medidas que procedan. Con el fin de aclarar estas novedades, la ley orgánica mantiene la misma denominación del Capítulo IV del Reglamento, dividiendo el articulado en cuatro capítulos dedicados, respectivamente, a las medidas generales de responsabilidad activa, al régimen del encargado del tratamiento, a la figura del delegado de protección de datos y a los mecanismos de autorregulación y certificación. La figura del delegado de protección de datos adquiere una destacada importancia en el Reglamento (UE) 2016/679 y así lo recoge la ley orgánica, que parte del principio de que puede tener un carácter obligatorio o voluntario, estar o no integrado en la organización del responsable o encargado y ser tanto una persona física como una persona jurídica. La designación del delegado de protección de datos ha de comunicarse a la autoridad de protección de datos competente. La Agencia Española de Protección de Datos mantendrá una relación pública y actualizada de los delegados de protección de datos, accesible por cualquier persona. Los conocimientos en la materia se podrán acreditar mediante esquemas de certificación. Asimismo, no podrá ser removido, salvo en los supuestos de dolo o negligencia grave. Es de destacar que el delegado de protección de datos permite configurar un medio para la resolución amistosa de reclamaciones, pues el interesado podrá reproducir ante él la reclamación que no sea atendida por el responsable o encargado del tratamiento.

El Título VI, relativo a las transferencias internacionales de datos, procede a la adaptación de lo previsto en el Reglamento (UE) 2016/679 y se refiere a las especialidades relacionadas con los procedimientos a través de los cuales las autoridades de protección de datos pueden aprobar modelos contractuales o normas corporativas vinculantes, supuestos de autorización de una determinada transferencia, o información previa.

El Título VII se dedica a las autoridades de protección de datos, que siguiendo el mandato del Reglamento (UE) 2016/679 se han de establecer por ley nacional. Manteniendo el esquema que se venía recogiendo en sus antecedentes normativos, la ley orgánica regula el régimen de la Agencia Española de Protección de Datos y refleja la existencia de las autoridades autonómicas de protección de datos y la necesaria cooperación entre las autoridades de control. La Agencia Española de Protección de Datos se configura como una autoridad administrativa independiente con arreglo a la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que se relaciona con el Gobierno a través del Ministerio de Justicia.

El Título VIII regula el «Procedimientos en caso de posible vulneración de la normativa de protección de datos». El Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. También se establece un procedimiento de cooperación entre autoridades de los Estados miembros y, en caso de

discrepancia, se prevé la decisión vinculante del Comité Europeo de Protección de Datos. En consecuencia, con carácter previo a la tramitación de cualquier procedimiento, será preciso determinar si el tratamiento tiene o no carácter transfronterizo y, en caso de tenerlo, qué autoridad de protección de datos ha de considerarse principal.

La regulación se limita a delimitar el régimen jurídico; la iniciación de los procedimientos, siendo posible que la Agencia Española de Protección de Datos remita la reclamación al delegado de protección de datos o a los órganos o entidades que tengan a su cargo la resolución extrajudicial de conflictos conforme a lo establecido en un código de conducta; la inadmisión de las reclamaciones; las actuaciones previas de investigación; las medidas provisionales, entre las que destaca la orden de bloqueo de los datos; y el plazo de tramitación de los procedimientos y, en su caso, su suspensión. Las especialidades del procedimiento se remiten al desarrollo reglamentario.

El Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación. En este marco, la ley orgánica procede a describir las conductas típicas, estableciendo la distinción entre infracciones muy graves, graves y leves, tomando en consideración la diferenciación que el Reglamento general de protección de datos establece al fijar la cuantía de las sanciones. La categorización de las infracciones se introduce a los solos efectos de determinar los plazos de prescripción, teniendo la descripción de las conductas típicas como único objeto la enumeración de manera ejemplificativa de algunos de los actos sancionables que deben entenderse incluidos dentro de los tipos generales establecidos en la norma europea. La ley orgánica regula los supuestos de interrupción de la prescripción partiendo de la exigencia constitucional del conocimiento de los hechos que se imputan a la persona, pero teniendo en cuenta la problemática derivada de los procedimientos establecidos en el reglamento europeo, en función de si el procedimiento se tramita exclusivamente por la Agencia Española de Protección de Datos o si se acude al procedimiento coordinado del artículo 60 del Reglamento general de protección de datos.

El Reglamento (UE) 2016/679 establece amplios márgenes para la determinación de la cuantía de las sanciones. La ley orgánica aprovecha la cláusula residual del artículo 83.2 de la norma europea, referida a los factores agravantes o atenuantes, para aclarar que entre los elementos a tener en cuenta podrán incluirse los que ya aparecían en el artículo 45.4 y 5 de la Ley Orgánica 15/1999, y que son conocidos por los operadores jurídicos.

Finalmente, el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. En particular, son objeto de regulación los derechos y libertades predicables al entorno de Internet como la neutralidad de la Red y el acceso universal o los derechos a la seguridad y educación digital así como los derechos al olvido, a la portabilidad y al testamento digital. Ocupa un lugar relevante el reconocimiento del derecho a la desconexión digital en el marco del derecho a la intimidad en el uso de dispositivos digitales en el ámbito laboral y la protección de los menores en Internet. Finalmente, resulta destacable la garantía de la libertad de expresión y el derecho a la aclaración de informaciones en medios de comunicación digitales.

Las disposiciones adicionales se refieren a cuestiones como las medidas de seguridad en el ámbito del sector público, protección de datos y transparencia y acceso a la información pública, cómputo de plazos, autorización judicial en materia de transferencias internacionales de datos, la protección frente a prácticas abusivas que pudieran desarrollar ciertos operadores, o los tratamientos de datos de salud, entre otras.

De conformidad con la disposición adicional decimocuarta, la normativa relativa a las excepciones y limitaciones en el ejercicio de los derechos que hubiese entrado en vigor con anterioridad a la fecha de aplicación del reglamento europeo y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, seguirá vigente en tanto no sea expresamente modificada, sustituida o derogada. La pervivencia de esta normativa supone la continuidad de las excepciones y limitaciones que en ella se contienen hasta que se produzca su reforma o abrogación, si bien referida a los derechos tal y como se regulan en el Reglamento (UE) 2016/679 y en esta ley orgánica. Así, por ejemplo, en virtud de la referida disposición adicional, las Administraciones

tributarias responsables de los ficheros de datos con trascendencia tributaria a que se refiere el artículo 95 de la Ley 58/2003, de 17 de diciembre, General Tributaria, podrán, en relación con dichos datos, denegar el ejercicio de los derechos a que se refieren los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

Las disposiciones transitorias están dedicadas, entre otras cuestiones, al estatuto de la Agencia Española de Protección de Datos, el régimen transitorio de los procedimientos o los tratamientos sometidos a la Directiva (UE) 2016/680. Se recoge una disposición derogatoria y, a continuación, figuran las disposiciones finales sobre los preceptos con carácter de ley ordinaria, el título competencial y la entrada en vigor.

Asimismo, se introducen las modificaciones necesarias de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, la Ley 14/1986, de 25 de abril, General de Sanidad, la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Finalmente, y en relación con la garantía de los derechos digitales, también se introducen modificaciones en la Ley Orgánica 2/2006, de 3 de mayo, de Educación, la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, así como en el Texto Refundido de la Ley del Estatuto de los Trabajadores y en el Texto Refundido de la Ley del Estatuto Básico del Empleado Público.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la ley.*

La presente ley orgánica tiene por objeto:

a) Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones.

El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica.

b) Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

Artículo 2. *Ámbito de aplicación de los Títulos I a IX y de los artículos 89 a 94.*

1. Lo dispuesto en los Títulos I a IX y en los artículos 89 a 94 de la presente ley orgánica se aplica a cualquier tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. Esta ley orgánica no será de aplicación:

a) A los tratamientos excluidos del ámbito de aplicación del Reglamento general de protección de datos por su artículo 2.2, sin perjuicio de lo dispuesto en los apartados 3 y 4 de este artículo.

b) A los tratamientos de datos de personas fallecidas, sin perjuicio de lo establecido en el artículo 3.

c) A los tratamientos sometidos a la normativa sobre protección de materias clasificadas.

3. Los tratamientos a los que no sea directamente aplicable el Reglamento (UE) 2016/679 por afectar a actividades no comprendidas en el ámbito de aplicación del Derecho de la Unión Europea, se regirán por lo dispuesto en su legislación específica si la hubiere y supletoriamente por lo establecido en el citado reglamento y en la presente ley orgánica. Se encuentran en esta situación, entre otros, los tratamientos realizados al amparo de la legislación orgánica del régimen electoral general, los tratamientos realizados en el ámbito de instituciones penitenciarias y los tratamientos derivados del Registro Civil, los Registros de la Propiedad y Mercantiles.

4. El tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente ley orgánica, sin perjuicio de las disposiciones de la Ley Orgánica 6/1985, de 1 julio, del Poder Judicial, que le sean aplicables.

5. El tratamiento de datos llevado a cabo con ocasión de la tramitación por el Ministerio Fiscal de los procesos de los que sea competente, así como el realizado con esos fines dentro de la gestión de la Oficina Fiscal, se regirán por lo dispuesto en el Reglamento (UE) 2016/679 y la presente Ley Orgánica, sin perjuicio de las disposiciones de la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal, la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y de las normas procesales que le sean aplicables.

Artículo 3. *Datos de las personas fallecidas.*

1. Las personas vinculadas al fallecido por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión.

Como excepción, las personas a las que se refiere el párrafo anterior no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los datos de carácter patrimonial del causante.

2. Las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión.

Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos.

3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

TÍTULO II

Principios de protección de datos

Artículo 4. *Exactitud de los datos.*

1. Conforme al artículo 5.1.d) del Reglamento (UE) 2016/679 los datos serán exactos y, si fuere necesario, actualizados.

2. A los efectos previstos en el artículo 5.1.d) del Reglamento (UE) 2016/679, no será imputable al responsable del tratamiento, siempre que este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación, la inexactitud de los datos personales, con respecto a los fines para los que se tratan, cuando los datos inexactos:

a) Hubiesen sido obtenidos por el responsable directamente del afectado.

b) Hubiesen sido obtenidos por el responsable de un mediador o intermediario en caso de que las normas aplicables al sector de actividad al que pertenezca el responsable del tratamiento establecieran la posibilidad de intervención de un intermediario o mediador que recoja en nombre propio los datos de los afectados para su transmisión al responsable. El mediador o intermediario asumirá las responsabilidades que pudieran derivarse en el supuesto de comunicación al responsable de datos que no se correspondan con los facilitados por el afectado.

c) Fuesen sometidos a tratamiento por el responsable por haberlos recibido de otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad conforme al artículo 20 del Reglamento (UE) 2016/679 y lo previsto en esta ley orgánica.

d) Fuesen obtenidos de un registro público por el responsable.

Artículo 5. *Deber de confidencialidad.*

1. Los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento.

Artículo 6. *Tratamiento basado en el consentimiento del afectado.*

1. De conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

2. Cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas.

3. No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

Artículo 7. *Consentimiento de los menores de edad.*

1. El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años.

Se exceptúan los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento.

2. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela.

Artículo 8. *Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.*

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley.

Artículo 9. *Categorías especiales de datos.*

1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.

Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

2. Los tratamientos de datos contemplados en las letras g), h) e i) del artículo 9.2 del Reglamento (UE) 2016/679 fundados en el Derecho español deberán estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad.

En particular, dicha norma podrá amparar el tratamiento de datos en el ámbito de la salud cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte.

Artículo 10. *Tratamiento de datos de naturaleza penal.*

1. El tratamiento de datos personales relativos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas, para fines distintos de los de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, solo podrá llevarse a cabo cuando se encuentre amparado en una norma de Derecho de la Unión, en esta ley orgánica o en otras normas de rango legal.

2. El registro completo de los datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas a que se refiere el artículo 10 del Reglamento (UE) 2016/679, podrá realizarse conforme con lo establecido en la regulación del Sistema de registros administrativos de apoyo a la Administración de Justicia.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a condenas e infracciones penales, así como a procedimientos y medidas cautelares y de seguridad conexas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO III

Derechos de las personas

CAPÍTULO I

Transparencia e información

Artículo 11. *Transparencia e información al afectado.*

1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

2. La información básica a la que se refiere el apartado anterior deberá contener, al menos:

a) La identidad del responsable del tratamiento y de su representante, en su caso.
b) La finalidad del tratamiento.
c) La posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que produzcan efectos jurídicos sobre él o le afecten significativamente de modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679.

3. Cuando los datos personales no hubieran sido obtenidos del afectado, el responsable podrá dar cumplimiento al deber de información establecido en el artículo 14 del Reglamento (UE) 2016/679 facilitando a aquel la información básica señalada en el apartado anterior, indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

En estos supuestos, la información básica incluirá también:

a) Las categorías de datos objeto de tratamiento.
b) Las fuentes de las que procedieran los datos.

CAPÍTULO II

Ejercicio de los derechos

Artículo 12. *Disposiciones generales sobre ejercicio de los derechos.*

1. Los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, podrán ejercerse directamente o por medio de representante legal o voluntario.

2. El responsable del tratamiento estará obligado a informar al afectado sobre los medios a su disposición para ejercer los derechos que le corresponden. Los medios deberán ser fácilmente accesibles para el afectado. El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio.

3. El encargado podrá tramitar, por cuenta del responsable, las solicitudes de ejercicio formuladas por los afectados de sus derechos si así se estableciere en el contrato o acto jurídico que les vincule.

4. La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de sus derechos formulado por el afectado recaerá sobre el responsable.

5. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el Capítulo III del Reglamento (UE) 2016/679, se estará a lo dispuesto en aquellas.

6. En cualquier caso, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la presente ley orgánica.

7. Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, sin perjuicio de lo dispuesto en los artículos 12.5 y 15.3 del Reglamento (UE) 2016/679 y en los apartados 3 y 4 del artículo 13 de esta ley orgánica.

Artículo 13. *Derecho de acceso.*

1. El derecho de acceso del afectado se ejercitará de acuerdo con lo establecido en el artículo 15 del Reglamento (UE) 2016/679.

Cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

2. El derecho de acceso se entenderá otorgado si el responsable del tratamiento facilitara al afectado un sistema de acceso remoto, directo y seguro a los datos personales

que garantice, de modo permanente, el acceso a su totalidad. A tales efectos, la comunicación por el responsable al afectado del modo en que este podrá acceder a dicho sistema bastará para tener por atendida la solicitud de ejercicio del derecho.

No obstante, el interesado podrá solicitar del responsable la información referida a los extremos previstos en el artículo 15.1 del Reglamento (UE) 2016/679 que no se incluyese en el sistema de acceso remoto.

3. A los efectos establecidos en el artículo 12.5 del Reglamento (UE) 2016/679 se podrá considerar repetitivo el ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.

4. Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas.

Artículo 14. *Derecho de rectificación.*

Al ejercer el derecho de rectificación reconocido en el artículo 16 del Reglamento (UE) 2016/679, el afectado deberá indicar en su solicitud a qué datos se refiere y la corrección que haya de realizarse. Deberá acompañar, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento.

Artículo 15. *Derecho de supresión.*

1. El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.

2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Artículo 16. *Derecho a la limitación del tratamiento.*

1. El derecho a la limitación del tratamiento se ejercerá de acuerdo con lo establecido en el artículo 18 del Reglamento (UE) 2016/679.

2. El hecho de que el tratamiento de los datos personales esté limitado debe constar claramente en los sistemas de información del responsable.

Artículo 17. *Derecho a la portabilidad.*

El derecho a la portabilidad se ejercerá de acuerdo con lo establecido en el artículo 20 del Reglamento (UE) 2016/679.

Artículo 18. *Derecho de oposición.*

El derecho de oposición, así como los derechos relacionados con las decisiones individuales automatizadas, incluida la realización de perfiles, se ejercerán de acuerdo con lo establecido, respectivamente, en los artículos 21 y 22 del Reglamento (UE) 2016/679.

TÍTULO IV

Disposiciones aplicables a tratamientos concretos

Artículo 19. *Tratamiento de datos de contacto, de empresarios individuales y de profesionales liberales.*

1. Salvo prueba en contrario, se presumirá amparado en lo dispuesto en el artículo 6.1.f) del Reglamento (UE) 2016/679 el tratamiento de los datos de contacto y en su caso los relativos a la función o puesto desempeñado de las personas físicas que presten servicios en una persona jurídica siempre que se cumplan los siguientes requisitos:

a) Que el tratamiento se refiera únicamente a los datos necesarios para su localización profesional.

b) Que la finalidad del tratamiento sea únicamente mantener relaciones de cualquier índole con la persona jurídica en la que el afectado preste sus servicios.

2. La misma presunción operará para el tratamiento de los datos relativos a los empresarios individuales y a los profesionales liberales, cuando se refieran a ellos únicamente en dicha condición y no se traten para entablar una relación con los mismos como personas físicas.

3. Los responsables o encargados del tratamiento a los que se refiere el artículo 77.1 de esta ley orgánica podrán también tratar los datos mencionados en los dos apartados anteriores cuando ello se derive de una obligación legal o sea necesario para el ejercicio de sus competencias.

Artículo 20. *Sistemas de información crediticia.*

1. Salvo prueba en contrario, se presumirá lícito el tratamiento de datos personales relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito por sistemas comunes de información crediticia cuando se cumplan los siguientes requisitos:

a) Que los datos hayan sido facilitados por el acreedor o por quien actúe por su cuenta o interés.

b) Que los datos se refieran a deudas ciertas, vencidas y exigibles, cuya existencia o cuantía no hubiese sido objeto de reclamación administrativa o judicial por el deudor o mediante un procedimiento alternativo de resolución de disputas vinculante entre las partes.

c) Que el acreedor haya informado al afectado en el contrato o en el momento de requerir el pago acerca de la posibilidad de inclusión en dichos sistemas, con indicación de aquéllos en los que participe.

La entidad que mantenga el sistema de información crediticia con datos relativos al incumplimiento de obligaciones dinerarias, financieras o de crédito deberá notificar al afectado la inclusión de tales datos y le informará sobre la posibilidad de ejercitar los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 dentro de los treinta días siguientes a la notificación de la deuda al sistema, permaneciendo bloqueados los datos durante ese plazo.

d) Que los datos únicamente se mantengan en el sistema mientras persista el incumplimiento, con el límite máximo de cinco años desde la fecha de vencimiento de la obligación dineraria, financiera o de crédito.

e) Que los datos referidos a un deudor determinado solamente puedan ser consultados cuando quien consulte el sistema mantuviese una relación contractual con el afectado que implique el abono de una cuantía pecuniaria o este le hubiera solicitado la celebración de un contrato que suponga financiación, pago aplazado o facturación periódica, como sucede, entre otros supuestos, en los previstos en la legislación de contratos de crédito al consumo y de contratos de crédito inmobiliario.

Cuando se hubiera ejercitado ante el sistema el derecho a la limitación del tratamiento de los datos impugnando su exactitud conforme a lo previsto en el artículo 18.1.a) del Reglamento (UE) 2016/679, el sistema informará a quienes pudieran consultarlo con arreglo al párrafo anterior acerca de la mera existencia de dicha circunstancia, sin facilitar los datos concretos respecto de los que se hubiera ejercitado el derecho, en tanto se resuelve sobre la solicitud del afectado.

f) Que, en el caso de que se denegase la solicitud de celebración del contrato, o éste no llegara a celebrarse, como consecuencia de la consulta efectuada, quien haya consultado el sistema informe al afectado del resultado de dicha consulta.

2. Las entidades que mantengan el sistema y las acreedoras, respecto del tratamiento de los datos referidos a sus deudores, tendrán la condición de corresponsables del tratamiento de los datos, siendo de aplicación lo establecido por el artículo 26 del Reglamento (UE) 2016/679.

Corresponderá al acreedor garantizar que concurren los requisitos exigidos para la inclusión en el sistema de la deuda, respondiendo de su inexistencia o inexactitud.

3. La presunción a la que se refiere el apartado 1 de este artículo no ampara los supuestos en que la información crediticia fuese asociada por la entidad que mantuviera el sistema a informaciones adicionales a las contempladas en dicho apartado, relacionadas con el deudor y obtenidas de otras fuentes, a fin de llevar a cabo un perfilado del mismo, en particular mediante la aplicación de técnicas de calificación crediticia.

Artículo 21. *Tratamientos relacionados con la realización de determinadas operaciones mercantiles.*

1. Salvo prueba en contrario, se presumirán lícitos los tratamientos de datos, incluida su comunicación con carácter previo, que pudieran derivarse del desarrollo de cualquier operación de modificación estructural de sociedades o la aportación o transmisión de negocio o de rama de actividad empresarial, siempre que los tratamientos fueran necesarios para el buen fin de la operación y garanticen, cuando proceda, la continuidad en la prestación de los servicios.

2. En el caso de que la operación no llegara a concluirse, la entidad cesionaria deberá proceder con carácter inmediato a la supresión de los datos, sin que sea de aplicación la obligación de bloqueo prevista en esta ley orgánica.

Artículo 22. *Tratamientos con fines de videovigilancia.*

1. Las personas físicas o jurídicas, públicas o privadas, podrán llevar a cabo el tratamiento de imágenes a través de sistemas de cámaras o videocámaras con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones.

2. Solo podrán captarse imágenes de la vía pública en la medida en que resulte imprescindible para la finalidad mencionada en el apartado anterior.

No obstante, será posible la captación de la vía pública en una extensión superior cuando fuese necesario para garantizar la seguridad de bienes o instalaciones estratégicos o de infraestructuras vinculadas al transporte, sin que en ningún caso pueda suponer la captación de imágenes del interior de un domicilio privado.

3. Los datos serán suprimidos en el plazo máximo de un mes desde su captación, salvo cuando hubieran de ser conservados para acreditar la comisión de actos que atenten contra la integridad de personas, bienes o instalaciones. En tal caso, las imágenes deberán ser puestas a disposición de la autoridad competente en un plazo máximo de setenta y dos horas desde que se tuviera conocimiento de la existencia de la grabación.

No será de aplicación a estos tratamientos la obligación de bloqueo prevista en el artículo 32 de esta ley orgánica.

4. El deber de información previsto en el artículo 12 del Reglamento (UE) 2016/679 se entenderá cumplido mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679. También podrá incluirse en el dispositivo informativo un código de conexión o dirección de internet a esta información.

En todo caso, el responsable del tratamiento deberá mantener a disposición de los afectados la información a la que se refiere el citado reglamento.

5. Al amparo del artículo 2.2.c) del Reglamento (UE) 2016/679, se considera excluido de su ámbito de aplicación el tratamiento por una persona física de imágenes que solamente capten el interior de su propio domicilio.

Esta exclusión no abarca el tratamiento realizado por una entidad de seguridad privada que hubiera sido contratada para la vigilancia de un domicilio y tuviese acceso a las imágenes.

6. El tratamiento de los datos personales procedentes de las imágenes y sonidos obtenidos mediante la utilización de cámaras y videocámaras por las Fuerzas y Cuerpos de Seguridad y por los órganos competentes para la vigilancia y control en los centros penitenciarios y para el control, regulación, vigilancia y disciplina del tráfico, se regirá por la legislación de transposición de la Directiva (UE) 2016/680, cuando el tratamiento tenga fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública. Fuera de estos supuestos, dicho tratamiento se regirá

por su legislación específica y supletoriamente por el Reglamento (UE) 2016/679 y la presente ley orgánica.

7. Lo regulado en el presente artículo se entiende sin perjuicio de lo previsto en la Ley 5/2014, de 4 de abril, de Seguridad Privada y sus disposiciones de desarrollo.

8. El tratamiento por el empleador de datos obtenidos a través de sistemas de cámaras o videocámaras se somete a lo dispuesto en el artículo 89 de esta ley orgánica.

Artículo 23. *Sistemas de exclusión publicitaria.*

1. Será lícito el tratamiento de datos personales que tenga por objeto evitar el envío de comunicaciones comerciales a quienes hubiesen manifestado su negativa u oposición a recibirlas.

A tal efecto, podrán crearse sistemas de información, generales o sectoriales, en los que solo se incluirán los datos imprescindibles para identificar a los afectados. Estos sistemas también podrán incluir servicios de preferencia, mediante los cuales los afectados limiten la recepción de comunicaciones comerciales a las procedentes de determinadas empresas.

2. Las entidades responsables de los sistemas de exclusión publicitaria comunicarán a la autoridad de control competente su creación, su carácter general o sectorial, así como el modo en que los afectados pueden incorporarse a los mismos y, en su caso, hacer valer sus preferencias.

La autoridad de control competente hará pública en su sede electrónica una relación de los sistemas de esta naturaleza que le fueran comunicados, incorporando la información mencionada en el párrafo anterior. A tal efecto, la autoridad de control competente a la que se haya comunicado la creación del sistema lo pondrá en conocimiento de las restantes autoridades de control para su publicación por todas ellas.

3. Cuando un afectado manifieste a un responsable su deseo de que sus datos no sean tratados para la remisión de comunicaciones comerciales, este deberá informarle de los sistemas de exclusión publicitaria existentes, pudiendo remitirse a la información publicada por la autoridad de control competente.

4. Quienes pretendan realizar comunicaciones de mercadotecnia directa, deberán previamente consultar los sistemas de exclusión publicitaria que pudieran afectar a su actuación, excluyendo del tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa al mismo. A estos efectos, para considerar cumplida la obligación anterior será suficiente la consulta de los sistemas de exclusión incluidos en la relación publicada por la autoridad de control competente.

No será necesario realizar la consulta a la que se refiere el párrafo anterior cuando el afectado hubiera prestado, conforme a lo dispuesto en esta ley orgánica, su consentimiento para recibir la comunicación a quien pretenda realizarla.

Artículo 24. *Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.*

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.

Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

Artículo 25. *Tratamiento de datos en el ámbito de la función estadística pública.*

1. El tratamiento de datos personales llevado a cabo por los organismos que tengan atribuidas las competencias relacionadas con el ejercicio de la función estadística pública se someterá a lo dispuesto en su legislación específica, así como en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

2. La comunicación de los datos a los órganos competentes en materia estadística solo se entenderá amparada en el artículo 6.1 e) del Reglamento (UE) 2016/679 en los casos en que la estadística para la que se requiera la información venga exigida por una norma de

Derecho de la Unión Europea o se encuentre incluida en los instrumentos de programación estadística legalmente previstos.

De conformidad con lo dispuesto en el artículo 11.2 de la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública, serán de aportación estrictamente voluntaria y, en consecuencia, solo podrán recogerse previo consentimiento expreso de los afectados los datos a los que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679.

3. Los organismos competentes para el ejercicio de la función estadística pública podrán denegar las solicitudes de ejercicio por los afectados de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 cuando los datos se encuentren amparados por las garantías del secreto estadístico previstas en la legislación estatal o autonómica.

Artículo 26. *Tratamiento de datos con fines de archivo en interés público por parte de las Administraciones Públicas.*

Será lícito el tratamiento por las Administraciones Públicas de datos con fines de archivo en interés público, que se someterá a lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica con las especialidades que se derivan de lo previsto en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español, en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación.

Artículo 27. *Tratamiento de datos relativos a infracciones y sanciones administrativas.*

1. A los efectos del artículo 86 del Reglamento (UE) 2016/679, el tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas, exigirá:

a) Que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, para la declaración de las infracciones o la imposición de las sanciones.

b) Que el tratamiento se limite a los datos estrictamente necesarios para la finalidad perseguida por aquel.

2. Cuando no se cumpla alguna de las condiciones previstas en el apartado anterior, los tratamientos de datos referidos a infracciones y sanciones administrativas habrán de contar con el consentimiento del interesado o estar autorizados por una norma con rango de ley, en la que se regularán, en su caso, garantías adicionales para los derechos y libertades de los afectados.

3. Fuera de los supuestos señalados en los apartados anteriores, los tratamientos de datos referidos a infracciones y sanciones administrativas solo serán posibles cuando sean llevados a cabo por abogados y procuradores y tengan por objeto recoger la información facilitada por sus clientes para el ejercicio de sus funciones.

TÍTULO V

Responsable y encargado del tratamiento

CAPÍTULO I

Disposiciones generales. Medidas de responsabilidad activa

Artículo 28. *Obligaciones generales del responsable y encargado del tratamiento.*

1. Los responsables y encargados, teniendo en cuenta los elementos enumerados en los artículos 24 y 25 del Reglamento (UE) 2016/679, determinarán las medidas técnicas y organizativas apropiadas que deben aplicar a fin de garantizar y acreditar que el tratamiento es conforme con el citado reglamento, con la presente ley orgánica, sus normas de desarrollo y la legislación sectorial aplicable. En particular valorarán si procede la realización

de la evaluación de impacto en la protección de datos y la consulta previa a que se refiere la Sección 3 del Capítulo IV del citado reglamento.

2. Para la adopción de las medidas a que se refiere el apartado anterior los responsables y encargados del tratamiento tendrán en cuenta, en particular, los mayores riesgos que podrían producirse en los siguientes supuestos:

a) Cuando el tratamiento pudiera generar situaciones de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico, moral o social significativo para los afectados.

b) Cuando el tratamiento pudiese privar a los afectados de sus derechos y libertades o pudiera impedirles el ejercicio del control sobre sus datos personales.

c) Cuando se produjese el tratamiento no meramente incidental o accesorio de las categorías especiales de datos a las que se refieren los artículos 9 y 10 del Reglamento (UE) 2016/679 y 9 y 10 de esta ley orgánica o de los datos relacionados con la comisión de infracciones administrativas.

d) Cuando el tratamiento implicase una evaluación de aspectos personales de los afectados con el fin de crear o utilizar perfiles personales de los mismos, en particular mediante el análisis o la predicción de aspectos referidos a su rendimiento en el trabajo, su situación económica, su salud, sus preferencias o intereses personales, su fiabilidad o comportamiento, su solvencia financiera, su localización o sus movimientos.

e) Cuando se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad y, en particular, de menores de edad y personas con discapacidad.

f) Cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales.

g) Cuando los datos personales fuesen a ser objeto de transferencia, con carácter habitual, a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección.

h) Cualesquiera otros que a juicio del responsable o del encargado pudieran tener relevancia y en particular aquellos previstos en códigos de conducta y estándares definidos por esquemas de certificación.

Artículo 29. *Supuestos de corresponsabilidad en el tratamiento.*

La determinación de las responsabilidades a las que se refiere el artículo 26.1 del Reglamento (UE) 2016/679 se realizará atendiendo a las actividades que efectivamente desarrolle cada uno de los corresponsables del tratamiento.

Artículo 30. *Representantes de los responsables o encargados del tratamiento no establecidos en la Unión Europea.*

1. En los supuestos en que el Reglamento (UE) 2016/679 sea aplicable a un responsable o encargado del tratamiento no establecido en la Unión Europea en virtud de lo dispuesto en su artículo 3.2 y el tratamiento se refiera a afectados que se hallen en España, la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos podrán imponer al representante, solidariamente con el responsable o encargado del tratamiento, las medidas establecidas en el Reglamento (UE) 2016/679.

Dicha exigencia se entenderá sin perjuicio de la responsabilidad que pudiera en su caso corresponder al responsable o al encargado del tratamiento y del ejercicio por el representante de la acción de repetición frente a quien proceda.

2. Asimismo, en caso de exigencia de responsabilidad en los términos previstos en el artículo 82 del Reglamento (UE) 2016/679, los responsables, encargados y representantes responderán solidariamente de los daños y perjuicios causados.

Artículo 31. *Registro de las actividades de tratamiento.*

1. Los responsables y encargados del tratamiento o, en su caso, sus representantes deberán mantener el registro de actividades de tratamiento al que se refiere el artículo 30 del

Reglamento (UE) 2016/679, salvo que sea de aplicación la excepción prevista en su apartado 5.

El registro, que podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento.

Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos deberán comunicarle cualquier adición, modificación o exclusión en el contenido del registro.

2. Los sujetos enumerados en el artículo 77.1 de esta ley orgánica harán público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal.

Artículo 32. *Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior.

4. Cuando para el cumplimiento de esta obligación, la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital, o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos durante el mismo.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, dentro del ámbito de sus respectivas competencias, podrán fijar excepciones a la obligación de bloqueo establecida en este artículo, en los supuestos en que, atendida la naturaleza de los datos o el hecho de que se refieran a un número particularmente elevado de afectados, su mera conservación, incluso bloqueados, pudiera generar un riesgo elevado para los derechos de los afectados, así como en aquellos casos en los que la conservación de los datos bloqueados pudiera implicar un coste desproporcionado para el responsable del tratamiento.

CAPÍTULO II

Encargado del tratamiento

Artículo 33. *Encargado del tratamiento.*

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

CAPÍTULO III

Delegado de protección de datos

Artículo 34. *Designación de un delegado de protección de datos.*

1. Los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades:

a) Los colegios profesionales y sus consejos generales.

b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas.

c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en su legislación específica, cuando traten habitual y sistemáticamente datos personales a gran escala.

d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

e) Las entidades incluidas en el artículo 1 de la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito.

f) Los establecimientos financieros de crédito.

g) Las entidades aseguradoras y reaseguradoras.

h) Las empresas de servicios de inversión, reguladas por la legislación del Mercado de Valores.

i) Los distribuidores y comercializadores de energía eléctrica y los distribuidores y comercializadores de gas natural.

j) Las entidades responsables de ficheros comunes para la evaluación de la solvencia patrimonial y crédito o de los ficheros comunes para la gestión y prevención del fraude, incluyendo a los responsables de los ficheros regulados por la legislación de prevención del blanqueo de capitales y de la financiación del terrorismo.

k) Las entidades que desarrollen actividades de publicidad y prospección comercial, incluyendo las de investigación comercial y de mercados, cuando lleven a cabo tratamientos basados en las preferencias de los afectados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

l) Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes.

Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de las historias clínicas de los pacientes, ejerzan su actividad a título individual.

m) Las entidades que tengan como uno de sus objetos la emisión de informes comerciales que puedan referirse a personas físicas.

n) Los operadores que desarrollen la actividad de juego a través de canales electrónicos, informáticos, telemáticos e interactivos, conforme a la normativa de regulación del juego.

ñ) Las empresas de seguridad privada.

o) Las federaciones deportivas cuando traten datos de menores de edad.

2. Los responsables o encargados del tratamiento no incluidos en el párrafo anterior podrán designar de manera voluntaria un delegado de protección de datos, que quedará sometido al régimen establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

3. Los responsables y encargados del tratamiento comunicarán en el plazo de diez días a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, las designaciones, nombramientos y ceses de los delegados de protección de datos tanto en los supuestos en que se encuentren obligadas a su designación como en el caso en que sea voluntaria.

4. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán, en el ámbito de sus respectivas competencias, una lista actualizada de delegados de protección de datos que será accesible por medios electrónicos.

5. En el cumplimiento de las obligaciones de este artículo los responsables y encargados del tratamiento podrán establecer la dedicación completa o a tiempo parcial del delegado, entre otros criterios, en función del volumen de los tratamientos, la categoría especial de los datos tratados o de los riesgos para los derechos o libertades de los interesados.

Artículo 35. *Cualificación del delegado de protección de datos.*

El cumplimiento de los requisitos establecidos en el artículo 37.5 del Reglamento (UE) 2016/679 para la designación del delegado de protección de datos, sea persona física o jurídica, podrá demostrarse, entre otros medios, a través de mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y la práctica en materia de protección de datos.

Artículo 36. *Posición del delegado de protección de datos.*

1. El delegado de protección de datos actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos. El delegado podrá inspeccionar los procedimientos relacionados con el objeto de la presente ley orgánica y emitir recomendaciones en el ámbito de sus competencias.

2. Cuando se trate de una persona física integrada en la organización del responsable o encargado del tratamiento, el delegado de protección de datos no podrá ser removido ni sancionado por el responsable o el encargado por desempeñar sus funciones salvo que incurriera en dolo o negligencia grave en su ejercicio. Se garantizará la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

3. En el ejercicio de sus funciones el delegado de protección de datos tendrá acceso a los datos personales y procesos de tratamiento, no pudiendo oponer a este acceso el responsable o el encargado del tratamiento la existencia de cualquier deber de confidencialidad o secreto, incluyendo el previsto en el artículo 5 de esta ley orgánica.

4. Cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento.

Artículo 37. *Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos.*

1. Cuando el responsable o el encargado del tratamiento hubieran designado un delegado de protección de datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su

caso, ante las autoridades autonómicas de protección de datos, dirigirse al delegado de protección de datos de la entidad contra la que se reclame.

En este caso, el delegado de protección de datos comunicará al afectado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación.

2. Cuando el afectado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, aquellas podrán remitir la reclamación al delegado de protección de datos a fin de que este responda en el plazo de un mes.

Si transcurrido dicho plazo el delegado de protección de datos no hubiera comunicado a la autoridad de protección de datos competente la respuesta dada a la reclamación, dicha autoridad continuará el procedimiento con arreglo a lo establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo.

3. El procedimiento ante la Agencia Española de Protección de Datos será el establecido en el Título VIII de esta ley orgánica y en sus normas de desarrollo. Asimismo, las comunidades autónomas regularán el procedimiento correspondiente ante sus autoridades autonómicas de protección de datos.

CAPÍTULO IV

Códigos de conducta y certificación

Artículo 38. *Códigos de conducta.*

1. Los códigos de conducta regulados por la sección 5.ª del Capítulo IV del Reglamento (UE) 2016/679 serán vinculantes para quienes se adhieran a los mismos.

Dichos códigos podrán dotarse de mecanismos de resolución extrajudicial de conflictos.

2. Dichos códigos podrán promoverse, además de por las asociaciones y organismos a los que se refiere el artículo 40.2 del Reglamento (UE) 2016/679, por empresas o grupos de empresas así como por los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica.

Asimismo, podrán ser promovidos por los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679.

Los responsables o encargados del tratamiento que se adhieran al código de conducta se obligan a someter al organismo o entidad de supervisión las reclamaciones que les fueran formuladas por los afectados en relación con los tratamientos de datos incluidos en su ámbito de aplicación en caso de considerar que no procede atender a lo solicitado en la reclamación, sin perjuicio de lo dispuesto en el artículo 37 de esta ley orgánica. Además, sin menoscabo de las competencias atribuidas por el Reglamento (UE) 2016/679 a las autoridades de protección de datos, podrán voluntariamente y antes de llevar a cabo el tratamiento, someter al citado organismo o entidad de supervisión la verificación de la conformidad del mismo con las materias sujetas al código de conducta.

En caso de que el organismo o entidad de supervisión rechace o desestime la reclamación, o si el responsable o encargado del tratamiento no somete la reclamación a su decisión, el afectado podrá formularla ante la Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos.

La autoridad de protección de datos competente verificará que los organismos o entidades que promuevan los códigos de conducta han dotado a estos códigos de organismos de supervisión que reúnan los requisitos establecidos en el artículo 41.2 del Reglamento (UE) 2016/679.

3. Los códigos de conducta serán aprobados por la Agencia Española de Protección de Datos o, en su caso, por la autoridad autonómica de protección de datos competente.

4. La Agencia Española de Protección de Datos o, en su caso, las autoridades autonómicas de protección de datos someterán los proyectos de código al mecanismo de coherencia mencionado en el artículo 63 de Reglamento (UE) 2016/679 en los supuestos en que ello proceda según su artículo 40.7. El procedimiento quedará suspendido en tanto el

Comité Europeo de Protección de Datos no emita el dictamen al que se refieren los artículos 64.1.b) y 65.1.c) del citado reglamento.

Cuando sea una autoridad autonómica de protección de datos la que someta el proyecto de código al mecanismo de coherencia, se estará a lo dispuesto en el artículo 60 de esta ley orgánica.

5. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos mantendrán registros de los códigos de conducta aprobados por las mismas, que estarán interconectados entre sí y coordinados con el registro gestionado por el Comité Europeo de Protección de Datos conforme al artículo 40.11 del citado reglamento.

El registro será accesible a través de medios electrónicos.

6. Mediante real decreto se establecerán el contenido del registro y las especialidades del procedimiento de aprobación de los códigos de conducta.

Artículo 39. *Acreditación de instituciones de certificación.*

Sin perjuicio de las funciones y poderes de acreditación de la autoridad de control competente en virtud de los artículos 57 y 58 del Reglamento (UE) 2016/679, la acreditación de las instituciones de certificación a las que se refiere el artículo 43.1 del citado reglamento podrá ser llevada a cabo por la Entidad Nacional de Acreditación (ENAC), que comunicará a la Agencia Española de Protección de Datos y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones de las acreditaciones, así como su motivación.

TÍTULO VI

Transferencias internacionales de datos

Artículo 40. *Régimen de las transferencias internacionales de datos.*

Las transferencias internacionales de datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y sus normas de desarrollo aprobadas por el Gobierno, y en las circulares de la Agencia Española de Protección de Datos y de las autoridades autonómicas de protección de datos, en el ámbito de sus respectivas competencias.

En todo caso se aplicarán a los tratamientos en que consista la propia transferencia las disposiciones contenidas en dichas normas, en particular las que regulan los principios de protección de datos.

Artículo 41. *Supuestos de adopción por la Agencia Española de Protección de Datos.*

1. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán adoptar, conforme a lo dispuesto en el artículo 46.2.c) del Reglamento (UE) 2016/679, cláusulas contractuales tipo para la realización de transferencias internacionales de datos, que se someterán previamente al dictamen del Comité Europeo de Protección de Datos previsto en el artículo 64 del citado reglamento.

2. La Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán aprobar normas corporativas vinculantes de acuerdo con lo previsto en el artículo 47 del Reglamento (UE) 2016/679.

El procedimiento se iniciará a instancia de una entidad situada en España y tendrá una duración máxima de nueve meses. Quedará suspendido como consecuencia de la remisión del expediente al Comité Europeo de Protección de Datos para que emita el dictamen al que se refiere el artículo 64.1.f) del Reglamento (UE) 2016/679, y continuará tras su notificación a la Agencia Española de Protección de Datos o a la autoridad autonómica de protección de datos competente.

Artículo 42. *Supuestos sometidos a autorización previa de las autoridades de protección de datos.*

1. Las transferencias internacionales de datos a países u organizaciones internacionales que no cuenten con decisión de adecuación aprobada por la Comisión o que no se amparen en alguna de las garantías previstas en el artículo anterior y en el artículo 46.2 del Reglamento (UE) 2016/679, requerirán una previa autorización de la Agencia Española de Protección de Datos o, en su caso, autoridades autonómicas de protección de datos, que podrá otorgarse en los siguientes supuestos:

a) Cuando la transferencia pretenda fundamentarse en la aportación de garantías adecuadas con fundamento en cláusulas contractuales que no correspondan a las cláusulas tipo previstas en el artículo 46.2, letras c) y d), del Reglamento (UE) 2016/679.

b) Cuando la transferencia se lleve a cabo por alguno de los responsables o encargados a los que se refiere el artículo 77.1 de esta ley orgánica y se funde en disposiciones incorporadas a acuerdos internacionales no normativos con otras autoridades u organismos públicos de terceros Estados, que incorporen derechos efectivos y exigibles para los afectados, incluidos los memorandos de entendimiento.

El procedimiento tendrá una duración máxima de seis meses.

2. La autorización quedará sometida a la emisión por el Comité Europeo de Protección de Datos del dictamen al que se refieren los artículos 64.1.e), 64.1.f) y 65.1.c) del Reglamento (UE) 2016/679. La remisión del expediente al citado comité implicará la suspensión del procedimiento hasta que el dictamen sea notificado a la Agencia Española de Protección de Datos o, por conducto de la misma, a la autoridad de control competente, en su caso.

Artículo 43. *Supuestos sometidos a información previa a la autoridad de protección de datos competente.*

Los responsables del tratamiento deberán informar a la Agencia Española de Protección de Datos o, en su caso, a las autoridades autonómicas de protección de datos, de cualquier transferencia internacional de datos que pretendan llevar a cabo sobre la base de su necesidad para fines relacionados con intereses legítimos imperiosos perseguidos por aquéllos y la concurrencia del resto de los requisitos previstos en el último párrafo del artículo 49.1 del Reglamento (UE) 2016/679. Asimismo, informarán a los afectados de la transferencia y de los intereses legítimos imperiosos perseguidos.

Esta información deberá facilitarse con carácter previo a la realización de la transferencia.

Lo dispuesto en este artículo no será de aplicación a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos, de acuerdo con el artículo 49.3 del Reglamento (UE) 2016/679.

TÍTULO VII

Autoridades de protección de datos

CAPÍTULO I

La Agencia Española de Protección de Datos

Sección 1.ª Disposiciones generales

Artículo 44. *Disposiciones generales.*

1. La Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones.

Su denominación oficial, de conformidad con lo establecido en el artículo 109.3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, será «Agencia Española de Protección de Datos, Autoridad Administrativa Independiente».

Se relaciona con el Gobierno a través del Ministerio de Justicia.

2. La Agencia Española de Protección de Datos tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos.

3. La Agencia Española de Protección de Datos, el Consejo General del Poder Judicial y en su caso, la Fiscalía General del Estado, colaborarán en aras del adecuado ejercicio de las respectivas competencias que la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, les atribuye en materia de protección de datos personales en el ámbito de la Administración de Justicia.

Artículo 45. *Régimen jurídico.*

1. La Agencia Española de Protección de Datos se rige por lo dispuesto en el Reglamento (UE) 2016/679, la presente ley orgánica y sus disposiciones de desarrollo.

Supletoriamente, en cuanto sea compatible con su plena independencia y sin perjuicio de lo previsto en el artículo 63.2 de esta ley orgánica, se regirá por las normas citadas en el artículo 110.1 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El Gobierno, a propuesta de la Agencia Española de Protección de Datos, aprobará su Estatuto mediante real decreto.

Artículo 46. *Régimen económico presupuestario y de personal.*

1. La Agencia Española de Protección de Datos elaborará y aprobará su presupuesto y lo remitirá al Gobierno para que sea integrado, con independencia, en los Presupuestos Generales del Estado.

2. El régimen de modificaciones y de vinculación de los créditos de su presupuesto será el establecido en el Estatuto de la Agencia Española de Protección de Datos.

Corresponde a la Presidencia de la Agencia Española de Protección de Datos autorizar las modificaciones presupuestarias que impliquen hasta un tres por ciento de la cifra inicial de su presupuesto total de gastos, siempre que no se incrementen los créditos para gastos de personal. Las restantes modificaciones que no excedan de un cinco por ciento del presupuesto serán autorizadas por el Ministerio de Hacienda y, en los demás casos, por el Gobierno.

3. La Agencia Española de Protección de Datos contará para el cumplimiento de sus fines con las asignaciones que se establezcan con cargo a los Presupuestos Generales del Estado, los bienes y valores que constituyan su patrimonio y los ingresos, ordinarios y extraordinarios derivados del ejercicio de sus actividades, incluidos los derivados del ejercicio de las potestades establecidos en el artículo 58 del Reglamento (UE) 2016/679.

4. El resultado positivo de sus ingresos se destinará por la Agencia Española de Protección de Datos a la dotación de sus reservas con el fin de garantizar su plena independencia.

5. El personal al servicio de la Agencia Española de Protección de Datos será funcionario o laboral y se regirá por lo previsto en el texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, y demás normativa reguladora de los funcionarios públicos y, en su caso, por la normativa laboral.

6. La Agencia Española de Protección Datos elaborará y aprobará su relación de puestos de trabajo, en el marco de los criterios establecidos por el Ministerio de Hacienda, respetando el límite de gasto de personal establecido en el presupuesto. En dicha relación de puestos de trabajo constarán, en todo caso, aquellos puestos que deban ser desempeñados en exclusiva por funcionarios públicos, por consistir en el ejercicio de las funciones que impliquen la participación directa o indirecta en el ejercicio de potestades públicas y la salvaguarda de los intereses generales del Estado y de las Administraciones Públicas.

7. Sin perjuicio de las competencias atribuidas al Tribunal de Cuentas, la gestión económico-financiera de la Agencia Española de Protección de Datos estará sometida al

control de la Intervención General de la Administración del Estado en los términos que establece la Ley 47/2003, de 26 de noviembre, General Presupuestaria.

Artículo 47. *Funciones y potestades de la Agencia Española de Protección de Datos.*

Corresponde a la Agencia Española de Protección de Datos supervisar la aplicación de esta ley orgánica y del Reglamento (UE) 2016/679 y, en particular, ejercer las funciones establecidas en el artículo 57 y las potestades previstas en el artículo 58 del mismo reglamento, en la presente ley orgánica y en sus disposiciones de desarrollo.

Asimismo, corresponde a la Agencia Española de Protección de Datos el desempeño de las funciones y potestades que le atribuyan otras leyes o normas de Derecho de la Unión Europea.

Artículo 48. *La Presidencia de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos la dirige, ostenta su representación y dicta sus resoluciones, circulares y directrices.

2. La Presidencia de la Agencia Española de Protección de Datos estará auxiliada por un Adjunto en el que podrá delegar sus funciones, a excepción de las relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica, y que la sustituirá en el ejercicio de las mismas en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Ambos ejercerán sus funciones con plena independencia y objetividad y no estarán sujetos a instrucción alguna en su desempeño. Les será aplicable la legislación reguladora del ejercicio del alto cargo de la Administración General del Estado.

En los supuestos de ausencia, vacante o enfermedad de la persona titular de la Presidencia o cuando concurran en ella alguno de los motivos de abstención o recusación previstos en el artículo 23 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el ejercicio de las competencias relacionadas con los procedimientos regulados por el título VIII de esta ley orgánica serán asumidas por la persona titular del órgano directivo que desarrolle las funciones de inspección. En el supuesto de que cualquiera de las circunstancias mencionadas concurriera igualmente en dicha persona, el ejercicio de las competencias afectadas será asumido por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

El ejercicio del resto de competencias será asumido por el Adjunto en los términos previstos en el Estatuto Orgánico de la Agencia Española de Protección de Datos y, en su defecto, por las personas titulares de los órganos directivos con nivel de subdirección general, por el orden establecido en el Estatuto.

3. La Presidencia de la Agencia Española de Protección de Datos y su Adjunto serán nombrados por el Gobierno, a propuesta del Ministerio de Justicia, entre personas de reconocida competencia profesional, en particular en materia de protección de datos.

Dos meses antes de producirse la expiración del mandato o, en el resto de las causas de cese, cuando se haya producido éste, el Ministerio de Justicia ordenará la publicación en el Boletín Oficial del Estado de la convocatoria pública de candidatos.

Previa evaluación del mérito, capacidad, competencia e idoneidad de los candidatos, el Gobierno remitirá al Congreso de los Diputados una propuesta de Presidencia y Adjunto acompañada de un informe justificativo que, tras la celebración de la preceptiva audiencia de los candidatos, deberá ser ratificada por la Comisión de Justicia en votación pública por mayoría de tres quintos de sus miembros en primera votación o, de no alcanzarse ésta, por mayoría absoluta en segunda votación, que se realizará inmediatamente después de la primera. En este último supuesto, los votos favorables deberán proceder de Diputados pertenecientes, al menos, a dos grupos parlamentarios diferentes.

4. La Presidencia y el Adjunto de la Agencia Española de Protección de Datos serán nombrados por el Consejo de Ministros mediante real decreto.

5. El mandato de la Presidencia y del Adjunto de la Agencia Española de Protección de Datos tiene una duración de cinco años y puede ser renovado para otro período de igual duración.

La Presidencia y el Adjunto solo cesarán antes de la expiración de su mandato, a petición propia o por separación acordada por el Consejo de Ministros, por:

a) Incumplimiento grave de sus obligaciones,
b) incapacidad sobrevenida para el ejercicio de su función,
c) incompatibilidad, o
d) condena firme por delito doloso.

En los supuestos previstos en las letras a), b) y c) será necesaria la ratificación de la separación por las mayorías parlamentarias previstas en el apartado 3 de este artículo.

6. Los actos y disposiciones dictados por la Presidencia de la Agencia Española de Protección de Datos ponen fin a la vía administrativa, siendo recurribles, directamente, ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional.

Artículo 49. *Consejo Consultivo de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos estará asesorada por un Consejo Consultivo compuesto por los siguientes miembros:

a) Un Diputado, propuesto por el Congreso de los Diputados.
b) Un Senador, propuesto por el Senado.
c) Un representante designado por el Consejo General del Poder Judicial.
d) Un representante de la Administración General del Estado con experiencia en la materia, propuesto por el Ministro de Justicia.
e) Un representante de cada Comunidad Autónoma que haya creado una Autoridad de protección de datos en su ámbito territorial, propuesto de acuerdo con lo que establezca la respectiva Comunidad Autónoma.
f) Un experto propuesto por la Federación Española de Municipios y Provincias.
g) Un experto propuesto por el Consejo de Consumidores y Usuarios.
h) Dos expertos propuestos por las Organizaciones Empresariales.
i) Un representante de los profesionales de la protección de datos y de la privacidad, propuesto por la asociación de ámbito estatal con mayor número de asociados.
j) Un representante de los organismos o entidades de supervisión y resolución extrajudicial de conflictos previstos en el Capítulo IV del Título V, propuesto por el Ministro de Justicia.
k) Un experto, propuesto por la Conferencia de Rectores de las Universidades Españolas.
l) Un representante de las organizaciones que agrupan a los Consejos Generales, Superiores y Colegios Profesionales de ámbito estatal de las diferentes profesiones colegiadas, propuesto por el Ministro de Justicia.
m) Un representante de los profesionales de la seguridad de la información, propuesto por la asociación de ámbito estatal con mayor número de asociados.
n) Un experto en transparencia y acceso a la información pública propuesto por el Consejo de Transparencia y Buen Gobierno.
ñ) Dos expertos propuestos por las organizaciones sindicales más representativas.

2. A los efectos del apartado anterior, la condición de experto requerirá acreditar conocimientos especializados en el Derecho y la práctica en materia de protección de datos mediante el ejercicio profesional o académico.

3. Los miembros del Consejo Consultivo serán nombrados por orden del Ministro de Justicia, publicada en el Boletín Oficial del Estado.

4. El Consejo Consultivo se reunirá cuando así lo disponga la Presidencia de la Agencia Española de Protección de Datos y, en todo caso, una vez al semestre.

5. Las decisiones tomadas por el Consejo Consultivo no tendrán en ningún caso carácter vinculante.

6. En todo lo no previsto por esta ley orgánica, el régimen, competencias y funcionamiento del Consejo Consultivo serán los establecidos en el Estatuto Orgánico de la Agencia Española de Protección de Datos.

Artículo 50. *Publicidad.*

La Agencia Española de Protección de Datos publicará las resoluciones de su Presidencia que declaren haber lugar o no a la atención de los derechos reconocidos en los

artículos 15 a 22 del Reglamento (UE) 2016/679, las que pongan fin a los procedimientos sancionadores y a los procedimientos de apercibimiento, las que archiven las actuaciones previas de investigación, las dictadas respecto de las entidades a que se refiere el artículo 77.1 de esta ley orgánica, las que impongan medidas cautelares y las demás que disponga su Estatuto.

Sección 2.ª Potestades de investigación y planes de auditoría preventiva

Artículo 51. *Ámbito y personal competente.*

1. La Agencia Española de Protección de Datos desarrollará su actividad de investigación a través de las actuaciones previstas en el Título VIII y de los planes de auditoría preventivas.

2. La actividad de investigación se llevará a cabo por los funcionarios de la Agencia Española de Protección de Datos o por funcionarios ajenos a ella habilitados expresamente por su Presidencia.

3. En los casos de actuaciones conjuntas de investigación conforme a lo dispuesto en el artículo 62 del Reglamento (UE) 2016/679, el personal de las autoridades de control de otros Estados Miembros de Unión Europea que colabore con la Agencia Española de Protección de Datos ejercerá sus facultades con arreglo a lo previsto en la presente ley orgánica y bajo la orientación y en presencia del personal de esta.

4. Los funcionarios que desarrollen actividades de investigación tendrán la consideración de agentes de la autoridad en el ejercicio de sus funciones, y estarán obligados a guardar secreto sobre las informaciones que conozcan con ocasión de dicho ejercicio, incluso después de haber cesado en él.

Artículo 52. *Deber de colaboración.*

1. Las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, y los particulares estarán obligados a proporcionar a la Agencia Española de Protección de Datos los datos, informes, antecedentes y justificantes necesarios para llevar a cabo su actividad de investigación.

Cuando la información contenga datos personales la comunicación de dichos datos estará amparada por lo dispuesto en el artículo 6.1 c) del Reglamento (UE) 2016/679.

2. En el marco de las actuaciones previas de investigación, cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de las Administraciones Públicas, incluidas las tributarias y de la Seguridad Social, las informaciones y datos que resulten imprescindibles con la exclusiva finalidad de lograr la identificación de los responsables de las conductas que pudieran ser constitutivas de infracción del Reglamento (UE) 2016/679 y de la presente ley orgánica.

En el supuesto de las Administraciones tributarias y de la Seguridad Social, la información se limitará a la que resulte necesaria para poder identificar inequívocamente contra quién debe dirigirse la actuación de la Agencia Española de Protección de Datos en los supuestos de creación de entramados societarios que dificultasen el conocimiento directo del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica.

3. Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y a la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica. A tales efectos, los datos que la Agencia Española de Protección de Datos podrá recabar al amparo de este apartado son los siguientes:

a) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de telefonía fija o móvil:

1.º El número de teléfono de origen de la llamada en caso de que el mismo se hubiese ocultado.

2.º El nombre, número de documento identificativo y dirección del abonado o usuario registrado al que corresponda ese número de teléfono.

3.º La mera confirmación de que se ha realizado una llamada específica entre dos números en una determinada fecha y hora.

b) Cuando la conducta se hubiera realizado mediante la utilización de un servicio de la sociedad de la información:

1.º La identificación de la dirección de protocolo de Internet desde la que se hubiera llevado a cabo la conducta y la fecha y hora de su realización.

2.º Si la conducta se hubiese llevado a cabo mediante correo electrónico, la identificación de la dirección de protocolo de Internet desde la que se creó la cuenta de correo y la fecha y hora en que la misma fue creada.

3.º El nombre, número de documento identificativo y dirección del abonado o del usuario registrado al que se le hubiera asignado la dirección de Protocolo de Internet a la que se refieren los dos párrafos anteriores.

Estos datos deberán ser cedidos, previo requerimiento motivado de la Agencia Española de Protección de Datos, exclusivamente en el marco de actuaciones de investigación iniciadas como consecuencia de una denuncia presentada por un afectado respecto de una conducta de una persona jurídica o respecto a la utilización de sistemas que permitan la divulgación sin restricciones de datos personales. En el resto de los supuestos la cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales cuando resultara exigible.

Quedan excluidos de lo previsto en este apartado los datos de tráfico que los operadores estuviesen tratando con la exclusiva finalidad de dar cumplimiento a las obligaciones previstas en la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, cuya cesión solamente podrá tener lugar de acuerdo con lo dispuesto en ella, previa autorización judicial solicitada por alguno de los agentes facultados a los que se refiere el artículo 6 de dicha ley.

Artículo 53. *Alcance de la actividad de investigación.*

1. Quienes desarrollen la actividad de investigación podrán recabar las informaciones precisas para el cumplimiento de sus funciones, realizar inspecciones, requerir la exhibición o el envío de los documentos y datos necesarios, examinarlos en el lugar en que se encuentren depositados o en donde se lleven a cabo los tratamientos, obtener copia de ellos, inspeccionar los equipos físicos y lógicos y requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del tratamiento sujetos a investigación.

2. Cuando fuese necesario el acceso por el personal que desarrolla la actividad de investigación al domicilio constitucionalmente protegido del inspeccionado, será preciso contar con su consentimiento o haber obtenido la correspondiente autorización judicial.

3. Cuando se trate de órganos judiciales u oficinas judiciales el ejercicio de las facultades de inspección se efectuará a través y por mediación del Consejo General del Poder Judicial.

Artículo 53 bis. *Actuaciones de investigación a través de sistemas digitales.*

Las actuaciones de investigación podrán realizarse a través de sistemas digitales que, mediante la videoconferencia u otro sistema similar, permitan la comunicación bidireccional y simultánea de imagen y sonido, la interacción visual, auditiva y verbal entre la Agencia Española de Protección de Datos y el inspeccionado. Además, deben garantizar la transmisión y recepción seguras de los documentos e información que se intercambien, y, en su caso, recoger las evidencias necesarias y el resultado de las actuaciones realizadas asegurando su autoría, autenticidad e integridad.

La utilización de estos sistemas se producirá cuando lo determine la Agencia y requerirá la conformidad del inspeccionado en relación con su uso y con la fecha y hora de su desarrollo.

Artículo 54. *Planes de auditoría.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá acordar la realización de planes de auditoría preventiva, referidos a los tratamientos de un sector concreto de actividad. Tendrán por objeto el análisis del cumplimiento de las disposiciones del Reglamento (UE) 2016/679 y de la presente ley orgánica, a partir de la realización de actividades de investigación sobre entidades pertenecientes al sector inspeccionado o sobre los responsables objeto de la auditoría.

2. A resultas de los planes de auditoría, la Presidencia de la Agencia Española de Protección de Datos podrá dictar las directrices generales o específicas para un concreto responsable o encargado de los tratamientos precisas para asegurar la plena adaptación del sector o responsable al Reglamento (UE) 2016/679 y a la presente ley orgánica.

En la elaboración de dichas directrices la Presidencia de la Agencia Española de Protección de Datos podrá solicitar la colaboración de los organismos de supervisión de los códigos de conducta y de resolución extrajudicial de conflictos, si los hubiere.

3. Las directrices serán de obligado cumplimiento para el sector o responsable al que se refiera el plan de auditoría.

Sección 3.ª Otras potestades de la Agencia Española de Protección de Datos

Artículo 55. *Potestades de regulación. Circulares de la Agencia Española de Protección de Datos.*

1. La Presidencia de la Agencia Española de Protección de Datos podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, que se denominarán «Circulares de la Agencia Española de Protección de Datos».

2. Su elaboración se sujetará al procedimiento establecido en el Estatuto de la Agencia Española de Protección de Datos, que deberá prever los informes técnicos y jurídicos que fueran necesarios y la audiencia a los interesados.

3. Las circulares serán obligatorias una vez publicadas en el Boletín Oficial del Estado.

Artículo 56. *Acción exterior.*

1. Corresponde a la Agencia Española de Protección de Datos la titularidad y el ejercicio de las funciones relacionadas con la acción exterior del Estado en materia de protección de datos.

Asimismo a las comunidades autónomas, a través de las autoridades autonómicas de protección de datos, les compete ejercitar las funciones como sujetos de la acción exterior en el marco de sus competencias de conformidad con lo dispuesto en la Ley 2/2014, de 25 de marzo, de la Acción y del Servicio Exterior del Estado, así como celebrar acuerdos internacionales administrativos en ejecución y concreción de un tratado internacional y acuerdos no normativos con los órganos análogos de otros sujetos de derecho internacional, no vinculantes jurídicamente para quienes los suscriben, sobre materias de su competencia en el marco de la Ley 25/2014, de 27 de noviembre, de Tratados y otros Acuerdos Internacionales.

2. La Agencia Española de Protección de Datos es el organismo competente para la protección de las personas físicas en lo relativo al tratamiento de datos personales derivado de la aplicación de cualquier Convenio Internacional en el que sea parte el Reino de España que atribuya a una autoridad nacional de control esa competencia y la representante común de las autoridades de Protección de Datos en el Comité Europeo de Protección de Datos, conforme a lo dispuesto en el artículo 68.4 del Reglamento (UE) 2016/679.

La Agencia Española de Protección de Datos informará a las autoridades autonómicas de protección de datos acerca de las decisiones adoptadas en el Comité Europeo de Protección de Datos y recabará su parecer cuando se trate de materias de su competencia.

3. Sin perjuicio de lo dispuesto en el apartado 1, la Agencia Española de Protección de Datos:

a) Participará en reuniones y foros internacionales de ámbito distinto al de la Unión Europea establecidos de común acuerdo por las autoridades de control independientes en materia de protección de datos.

b) Participará, como autoridad española, en las organizaciones internacionales competentes en materia de protección de datos, en los comités o grupos de trabajo, de estudio y de colaboración de organizaciones internacionales que traten materias que afecten al derecho fundamental a la protección de datos personales y en otros foros o grupos de trabajo internacionales, en el marco de la acción exterior del Estado.

c) Colaborará con autoridades, instituciones, organismos y Administraciones de otros Estados a fin de impulsar, promover y desarrollar el derecho fundamental a la protección de datos, en particular en el ámbito iberoamericano, pudiendo suscribir acuerdos internacionales administrativos y no normativos en la materia.

CAPÍTULO II

Autoridades autonómicas de protección de datos

Sección 1.ª Disposiciones generales

Artículo 57. *Autoridades autonómicas de protección de datos.*

1. Las autoridades autonómicas de protección de datos personales podrán ejercer, las funciones y potestades establecidas en los artículos 57 y 58 del Reglamento (UE) 2016/679, de acuerdo con la normativa autonómica, cuando se refieran a:

a) Tratamientos de los que sean responsables las entidades integrantes del sector público de la correspondiente Comunidad Autónoma o de las Entidades Locales incluidas en su ámbito territorial o quienes presten servicios a través de cualquier forma de gestión directa o indirecta.

b) Tratamientos llevados a cabo por personas físicas o jurídicas para el ejercicio de las funciones públicas en materias que sean competencia de la correspondiente Administración Autonómica o Local.

c) Tratamientos que se encuentren expresamente previstos, en su caso, en los respectivos Estatutos de Autonomía.

2. Las autoridades autonómicas de protección de datos podrán dictar, en relación con los tratamientos sometidos a su competencia, circulares con el alcance y los efectos establecidos para la Agencia Española de Protección de Datos en el artículo 55 de esta ley orgánica.

Artículo 58. *Cooperación institucional.*

La Presidencia de la Agencia Española de Protección de Datos convocará, por iniciativa propia o cuando lo solicite otra autoridad, a las autoridades autonómicas de protección de datos para contribuir a la aplicación coherente del Reglamento (UE) 2016/679 y de la presente ley orgánica. En todo caso, se celebrarán reuniones semestrales de cooperación.

La Presidencia de la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos podrán solicitar y deberán intercambiarse mutuamente la información necesaria para el cumplimiento de sus funciones y, en particular, la relativa a la actividad del Comité Europeo de Protección de Datos. Asimismo, podrán constituir grupos de trabajo para tratar asuntos específicos de interés común.

Artículo 59. *Tratamientos contrarios al Reglamento (UE) 2016/679.*

Cuando la Presidencia de la Agencia Española de Protección de Datos considere que un tratamiento llevado a cabo en materias que fueran competencia de las autoridades autonómicas de protección de datos vulnera el Reglamento (UE) 2016/679 podrá requerirlas a que adopten, en el plazo de un mes, las medidas necesarias para su cesación.

Si la autoridad autonómica no atendiere en plazo el requerimiento o las medidas adoptadas no supusiesen la cesación en el tratamiento ilícito, la Agencia Española de

Protección de Datos podrá ejercer las acciones que procedan ante la jurisdicción contencioso-administrativa.

Sección 2.ª Coordinación en el marco de los procedimientos establecidos en el Reglamento (UE) 2016/679

Artículo 60. *Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos.*

Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando éstas, como autoridades competentes, deban someter su proyecto de decisión al citado comité o le soliciten el examen de un asunto en virtud de lo establecido en los apartados 1 y 2 del artículo 64 del Reglamento (UE) 2016/679.

En estos casos, la Agencia Española de Protección de Datos será asistida por un representante de la Autoridad autonómica en su intervención ante el Comité.

Artículo 61. *Intervención en caso de tratamientos transfronterizos.*

1. Las autoridades autonómicas de protección de datos ostentarán la condición de autoridad de control principal o interesada en el procedimiento establecido por el artículo 60 del Reglamento (UE) 2016/679 cuando se refiera a un tratamiento previsto en el artículo 57 de esta ley orgánica que se llevara a cabo por un responsable o encargado del tratamiento de los previstos en el artículo 56 del Reglamento (UE) 2016/679, salvo que desarrollase significativamente tratamientos de la misma naturaleza en el resto del territorio español.

2. Corresponderá en estos casos a las autoridades autonómicas intervenir en los procedimientos establecidos en el artículo 60 del Reglamento (UE) 2016/679, informando a la Agencia Española de Protección de Datos sobre su desarrollo en los supuestos en que deba aplicarse el mecanismo de coherencia.

Artículo 62. *Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos.*

1. Se practicarán por conducto de la Agencia Española de Protección de Datos todas las comunicaciones entre el Comité Europeo de Protección de Datos y las autoridades autonómicas de protección de datos cuando estas, como autoridades principales, deban solicitar del citado Comité la emisión de una decisión vinculante según lo previsto en el artículo 65 del Reglamento (UE) 2016/679.

2. Las autoridades autonómicas de protección de datos que tengan la condición de autoridad interesada no principal en un procedimiento de los previstos en el artículo 65 del Reglamento (UE) 2016/679 informarán a la Agencia Española de Protección de Datos cuando el asunto sea remitido al Comité Europeo de Protección de Datos, facilitándole la documentación e información necesarias para su tramitación.

La Agencia Española de Protección de Datos será asistida por un representante de la autoridad autonómica interesada en su intervención ante el mencionado comité.

TÍTULO VIII

Procedimientos en caso de posible vulneración de la normativa de protección de datos

Artículo 63. *Régimen jurídico.*

1. Las disposiciones de este Título serán de aplicación a los procedimientos tramitados por la Agencia Española de Protección de Datos en los supuestos en los que un afectado reclame que no ha sido atendida su solicitud de ejercicio de los derechos reconocidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, así como en los que aquella investigue la existencia de una posible infracción de lo dispuesto en el mencionado reglamento y en la presente ley orgánica.

2. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos.

3. El Gobierno regulará por real decreto los procedimientos que tramite la Agencia Española de Protección de Datos al amparo de este Título, asegurando en todo caso los derechos de defensa y audiencia de los interesados.

Artículo 64. *Forma de iniciación del procedimiento y duración.*

1. Cuando el procedimiento se refiera exclusivamente a la falta de atención de una solicitud de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se iniciará por acuerdo de admisión a trámite, que se adoptará conforme a lo establecido en el artículo 65 de esta ley orgánica.

En este caso el plazo para resolver el procedimiento será de seis meses a contar desde la fecha en que hubiera sido notificado al reclamante el acuerdo de admisión a trámite. Transcurrido ese plazo, el interesado podrá considerar estimada su reclamación.

2. Cuando el procedimiento tenga por objeto la determinación de la posible existencia de una infracción de lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la presente ley orgánica, se iniciará mediante acuerdo de inicio, adoptado por propia iniciativa o como consecuencia de reclamación, que le será notificado al interesado.

Si el procedimiento se fundase en una reclamación formulada ante la Agencia Española de Protección de Datos, con carácter previo, esta decidirá sobre su admisión a trámite, conforme a lo dispuesto en el artículo 65 de esta ley orgánica.

Admitida a trámite la reclamación, así como en los supuestos en que la Agencia Española de Protección de Datos actúe por propia iniciativa, con carácter previo al acuerdo de inicio podrá existir una fase de actuaciones previas de investigación, que se regirá por lo previsto en el artículo 67 de esta ley orgánica.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

3. Cuando así proceda en atención a la naturaleza de los hechos y teniendo debidamente en cuenta los criterios establecidos en el artículo 83.2 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la Agencia Española de Protección de Datos, previa audiencia al responsable o encargado del tratamiento, podrá dirigir un apercibimiento, así como ordenar al responsable o encargado del tratamiento que adopten las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos de una determinada manera y dentro del plazo especificado.

El procedimiento tendrá una duración máxima de seis meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones.

Será de aplicación en este caso lo dispuesto en los párrafos segundo y tercero del apartado 2 de este artículo.

4. El procedimiento podrá también tramitarse como consecuencia de la comunicación a la Agencia Española de Protección de Datos por parte de la autoridad de control de otro Estado miembro de la Unión Europea de la reclamación formulada ante la misma, cuando la Agencia Española de Protección de Datos tuviese la condición de autoridad de control principal para la tramitación de un procedimiento conforme a lo dispuesto en los artículos 56 y 60 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Será en este caso de aplicación lo dispuesto en los apartados 1, 2 y 3 de este artículo.

5. Los plazos de tramitación establecidos en este artículo así como los de admisión a trámite regulados por el artículo 65.5 y de duración de las actuaciones previas de investigación previstos en el artículo 67.2, quedarán automáticamente suspendidos cuando deba recabarse información, consulta, solicitud de asistencia o pronunciamiento preceptivo de un órgano u organismo de la Unión Europea o de una o varias autoridades de control de

los Estados miembros conforme con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos.

6. El transcurso de los plazos de tramitación a los que se refiere el apartado anterior se podrá suspender, mediante resolución motivada, cuando resulte indispensable recabar información de un órgano jurisdiccional.

Artículo 65. *Admisión a trámite de las reclamaciones.*

1. Cuando se presentase ante la Agencia Española de Protección de Datos una reclamación, esta deberá evaluar su admisibilidad a trámite, de conformidad con las previsiones de este artículo.

2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos personales, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción.

3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia Española de Protección de Datos, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias:

a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica.

b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas.

4. Antes de resolver sobre la admisión a trámite de la reclamación, la Agencia Española de Protección de Datos podrá remitir la misma al delegado de protección de datos que hubiera, en su caso, designado el responsable o encargado del tratamiento, al organismo de supervisión establecido para la aplicación de los códigos de conducta o al organismo que asuma las funciones de resolución extrajudicial de conflictos a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica.

La Agencia Española de Protección de Datos podrá igualmente remitir la reclamación al responsable o encargado del tratamiento cuando no se hubiera designado un delegado de protección de datos ni estuviera adherido a mecanismos de resolución extrajudicial de conflictos, en cuyo caso el responsable o encargado deberá dar respuesta a la reclamación en el plazo de un mes.

Si como consecuencia de dichas actuaciones de remisión, el responsable o encargado del tratamiento demuestra haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá inadmitir a trámite la reclamación.

5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si transcurrido este plazo no se produjera dicha notificación, se entenderá que prosigue la tramitación de la reclamación con arreglo a lo dispuesto en este título a partir de la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos, sin perjuicio de la facultad de la Agencia de archivar posteriormente y de forma expresa la reclamación.

En el supuesto de que la Agencia Española de Protección de Datos actúe como consecuencia de la comunicación que le hubiera sido remitida por la autoridad de control de otro Estado miembro de la Unión Europea, conforme al artículo 64.4 de esta ley orgánica, el cómputo del plazo señalado en el párrafo anterior se iniciará una vez que se reciba en la Agencia toda la documentación necesaria para su tramitación.

Cuando los hechos de una reclamación relativa a la posible existencia en el ámbito competencial de la Agencia, guarden identidad sustancial con los que sean objeto de unas actuaciones previas de investigación o de un procedimiento sancionador ya iniciado, en la notificación de la decisión de admisión a trámite se podrá indicar el número de expediente

correspondiente a las actuaciones previas o al procedimiento correspondiente, así como de la dirección web en la que se publicará la resolución que ponga fin al mismo, a efectos de que el reclamante pueda conocer el curso y resultado de la investigación.

6. Tras la admisión a trámite, si el responsable o encargado del tratamiento demuestran haber adoptado medidas para el cumplimiento de la normativa aplicable, la Agencia Española de Protección de Datos podrá resolver el archivo de la reclamación, cuando en el caso concreto concurran circunstancias que aconsejen la adopción de otras soluciones más moderadas o alternativas a la acción correctiva, siempre que no se hayan iniciado actuaciones previas de investigación o alguno de los procedimientos regulados en esta ley orgánica.

Artículo 66. *Determinación del alcance territorial.*

1. Salvo en los supuestos a los que se refiere el artículo 64.4 de esta ley orgánica, la Agencia Española de Protección de Datos deberá, con carácter previo a la realización de cualquier otra actuación, incluida la admisión a trámite de una reclamación o el comienzo de actuaciones previas de investigación, examinar su competencia y determinar el carácter nacional o transfronterizo, en cualquiera de sus modalidades, del procedimiento a seguir.

2. Si la Agencia Española de Protección de Datos considera que no tiene la condición de autoridad de control principal para la tramitación del procedimiento remitirá, sin más trámite, la reclamación formulada a la autoridad de control principal que considere competente, a fin de que por la misma se le dé el curso oportuno. La Agencia Española de Protección de Datos notificará esta circunstancia a quien, en su caso, hubiera formulado la reclamación.

El acuerdo por el que se resuelva la remisión a la que se refiere el párrafo anterior implicará el archivo provisional del procedimiento, sin perjuicio de que por la Agencia Española de Protección de Datos se dicte, en caso de que así proceda, la resolución a la que se refiere el apartado 8 del artículo 60 del Reglamento (UE) 2016/679.

Artículo 67. *Actuaciones previas de investigación.*

1. Antes de la adopción del acuerdo de inicio de procedimiento, y una vez admitida a trámite la reclamación si la hubiese, la Agencia Española de Protección de Datos podrá llevar a cabo actuaciones previas de investigación a fin de lograr una mejor determinación de los hechos y las circunstancias que justifican la tramitación del procedimiento.

La Agencia Española de Protección de Datos actuará en todo caso cuando sea precisa la investigación de tratamientos que implique un tráfico masivo de datos personales.

2. Las actuaciones previas de investigación se someterán a lo dispuesto en la sección 2.ª del capítulo I del título VII de esta ley orgánica y no podrán tener una duración superior a dieciocho meses a contar desde la fecha del acuerdo de admisión a trámite o de la fecha del acuerdo por el que se decida su iniciación cuando la Agencia Española de Protección de Datos actúe por propia iniciativa.

Artículo 68. *Acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionadora.*

1. Concluidas, en su caso, las actuaciones a las que se refiere el artículo anterior, corresponderá a la Presidencia de la Agencia Española de Protección de Datos, cuando así proceda, dictar acuerdo de inicio de procedimiento para el ejercicio de la potestad sancionadora, en que se concretarán los hechos, la identificación de la persona o entidad contra la que se dirija el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

2. Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679, el proyecto de acuerdo de inicio de procedimiento sancionador se someterá a lo dispuesto en el mismo.

Artículo 69. *Medidas provisionales y de garantía de los derechos.*

1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de

Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.

2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportara un menoscabo grave del derecho a la protección de datos personales, podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización.

3. Cuando se hubiese presentado ante la Agencia Española de Protección de Datos una reclamación que se refiriese, entre otras cuestiones, a la falta de atención en plazo de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, la Agencia Española de Protección de Datos podrá acordar en cualquier momento, incluso con anterioridad a la iniciación del procedimiento para el ejercicio de la potestad sancionadora, mediante resolución motivada y previa audiencia del responsable del tratamiento, la obligación de atender el derecho solicitado, prosiguiéndose el procedimiento en cuanto al resto de las cuestiones objeto de la reclamación.

TÍTULO IX

Régimen sancionador

Artículo 70. *Sujetos responsables.*

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos.
b) Los encargados de los tratamientos.
c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.
d) Las entidades de certificación.
e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título.

Artículo 71. *Infracciones.*

Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica.

Artículo 72. *Infracciones consideradas muy graves.*

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679.
b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.
c) El incumplimiento de los requisitos exigidos por el artículo 7 del Reglamento (UE) 2016/679 para la validez del consentimiento.
d) La utilización de los datos para una finalidad que no sea compatible con la finalidad para la cual fueron recogidos, sin contar con el consentimiento del afectado o con una base legal para ello.

e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.

f) El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas fuera de los supuestos permitidos por el artículo 10 del Reglamento (UE) 2016/679 y en el artículo 10 de esta ley orgánica.

g) El tratamiento de datos personales relacionados con infracciones y sanciones administrativas fuera de los supuestos permitidos por el artículo 27 de esta ley orgánica.

h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica.

i) La vulneración del deber de confidencialidad establecido en el artículo 5 de esta ley orgánica.

j) La exigencia del pago de un canon para facilitar al afectado la información a la que se refieren los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, fuera de los supuestos establecidos en su artículo 12.5.

k) El impedimento o la obstaculización o la no atención reiterada del ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.

l) La transferencia internacional de datos personales a un destinatario que se encuentre en un tercer país o a una organización internacional, cuando no concurran las garantías, requisitos o excepciones establecidos en los artículos 44 a 49 del Reglamento (UE) 2016/679.

m) El incumplimiento de las resoluciones dictadas por la autoridad de protección de datos competente en ejercicio de los poderes que le confiere el artículo 58.2 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de bloqueo de los datos establecida en el artículo 32 de esta ley orgánica cuando la misma sea exigible.

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente.

p) La reversión deliberada de un procedimiento de anonimización a fin de permitir la reidentificación de los afectados.

2. Tendrán la misma consideración y también prescribirán a los tres años las infracciones a las que se refiere el artículo 83.6 del Reglamento (UE) 2016/679.

Artículo 73. *Infracciones consideradas graves.*

En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales de un menor de edad sin recabar su consentimiento, cuando tenga capacidad para ello, o el del titular de su patria potestad o tutela, conforme al artículo 8 del Reglamento (UE) 2016/679.

b) No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad o por el titular de su patria potestad o tutela sobre el mismo, conforme a lo requerido por el artículo 8.2 del Reglamento (UE) 2016/679.

c) El impedimento o la obstaculización o la no atención reiterada de los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación.

d) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el

diseño, así como la no integración de las garantías necesarias en el tratamiento, en los términos exigidos por el artículo 25 del Reglamento (UE) 2016/679.

e) La falta de adopción de las medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratarán los datos personales necesarios para cada uno de los fines específicos del tratamiento, conforme a lo exigido por el artículo 25.2 del Reglamento (UE) 2016/679.

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679.

h) El incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no establecido en el territorio de la Unión Europea, conforme a lo previsto en el artículo 27 del Reglamento (UE) 2016/679.

i) La falta de atención por el representante en la Unión del responsable o del encargado del tratamiento de las solicitudes efectuadas por la autoridad de protección de datos o por los afectados.

j) La contratación por el responsable del tratamiento de un encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas conforme a lo establecido en el Capítulo IV del Reglamento (UE) 2016/679.

k) Encargar el tratamiento de datos a un tercero sin la previa formalización de un contrato u otro acto jurídico escrito con el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.

l) La contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable, o sin haberle informado sobre los cambios producidos en la subcontratación cuando fueran legalmente exigibles.

m) La infracción por un encargado del tratamiento de lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica, al determinar los fines y los medios del tratamiento, conforme a lo dispuesto en el artículo 28.10 del citado reglamento.

n) No disponer del registro de actividades de tratamiento establecido en el artículo 30 del Reglamento (UE) 2016/679.

ñ) No poner a disposición de la autoridad de protección de datos que lo haya solicitado, el registro de actividades de tratamiento, conforme al apartado 4 del artículo 30 del Reglamento (UE) 2016/679.

o) No cooperar con las autoridades de control en el desempeño de sus funciones en los supuestos no previstos en el artículo 72 de esta ley orgánica.

p) El tratamiento de datos personales sin llevar a cabo una previa valoración de los elementos mencionados en el artículo 28 de esta ley orgánica.

q) El incumplimiento del deber del encargado del tratamiento de notificar al responsable del tratamiento las violaciones de seguridad de las que tuviera conocimiento.

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

u) El tratamiento de datos personales sin haber consultado previamente a la autoridad de protección de datos en los casos en que dicha consulta resulta preceptiva conforme al artículo 36 del Reglamento (UE) 2016/679 o cuando la ley establezca la obligación de llevar a cabo esa consulta.

v) El incumplimiento de la obligación de designar un delegado de protección de datos cuando sea exigible su nombramiento de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

w) No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales, no respaldarlo o interferir en el desempeño de sus funciones.

x) La utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación debidamente acreditada o en caso de que la vigencia del mismo hubiera expirado.

y) Obtener la acreditación como organismo de certificación presentando información inexacta sobre el cumplimiento de los requisitos exigidos por el artículo 43 del Reglamento (UE) 2016/679.

z) El desempeño de funciones que el Reglamento (UE) 2016/679 reserva a los organismos de certificación, sin haber sido debidamente acreditado conforme a lo establecido en el artículo 39 de esta ley orgánica.

aa) El incumplimiento por parte de un organismo de certificación de los principios y deberes a los que está sometido según lo previsto en los artículos 42 y 43 de Reglamento (UE) 2016/679.

ab) El desempeño de funciones que el artículo 41 del Reglamento (UE) 2016/679 reserva a los organismos de supervisión de códigos de conducta sin haber sido previamente acreditado por la autoridad de protección de datos competente.

ac) La falta de adopción por parte de los organismos acreditados de supervisión de un código de conducta de las medidas que resulten oportunas en caso que se hubiera producido una infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 74. *Infracciones consideradas leves.*

Se consideran leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:

a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.

b) La exigencia del pago de un canon para facilitar al afectado la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679 o por atender las solicitudes de ejercicio de derechos de los afectados previstos en los artículos 15 a 22 del Reglamento (UE) 2016/679, cuando así lo permita su artículo 12.5, si su cuantía excediese el importe de los costes afrontados para facilitar la información o realizar la actuación solicitada.

c) No atender las solicitudes de ejercicio de los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679, salvo que resultase de aplicación lo dispuesto en el artículo 72.1.k) de esta ley orgánica.

d) No atender los derechos de acceso, rectificación, supresión, limitación del tratamiento o a la portabilidad de los datos en tratamientos en los que no se requiere la identificación del afectado, cuando este, para el ejercicio de esos derechos, haya facilitado información adicional que permita su identificación, salvo que resultase de aplicación lo dispuesto en el artículo 73 c) de esta ley orgánica.

e) El incumplimiento de la obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento exigida por el artículo 19 del Reglamento (UE) 2016/679.

f) El incumplimiento de la obligación de informar al afectado, cuando así lo haya solicitado, de los destinatarios a los que se hayan comunicado los datos personales rectificados, suprimidos o respecto de los que se ha limitado el tratamiento.

g) El incumplimiento de la obligación de suprimir los datos referidos a una persona fallecida cuando ello fuera exigible conforme al artículo 3 de esta ley orgánica.

h) La falta de formalización por los corresponsables del tratamiento del acuerdo que determine las obligaciones, funciones y responsabilidades respectivas con respecto al

tratamiento de datos personales y sus relaciones con los afectados al que se refiere el artículo 26 del Reglamento (UE) 2016/679 o la inexactitud en la determinación de las mismas.

i) No poner a disposición de los afectados los aspectos esenciales del acuerdo formalizado entre los corresponsables del tratamiento, conforme exige el artículo 26.2 del Reglamento (UE) 2016/679.

j) La falta del cumplimiento de la obligación del encargado del tratamiento de informar al responsable del tratamiento acerca de la posible infracción por una instrucción recibida de este de las disposiciones del Reglamento (UE) 2016/679 o de esta ley orgánica, conforme a lo exigido por el artículo 28.3 del citado reglamento.

k) El incumplimiento por el encargado de las estipulaciones impuestas en el contrato o acto jurídico que regula el tratamiento o las instrucciones del responsable del tratamiento, salvo que esté legalmente obligado a ello conforme al Reglamento (UE) 2016/679 y a la presente ley orgánica o en los supuestos en que fuese necesario para evitar la infracción de la legislación en materia de protección de datos y se hubiese advertido de ello al responsable o al encargado del tratamiento.

l) Disponer de un Registro de actividades de tratamiento que no incorpore toda la información exigida por el artículo 30 del Reglamento (UE) 2016/679.

m) La notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

n) El incumplimiento de la obligación de documentar cualquier violación de seguridad, exigida por el artículo 33.5 del Reglamento (UE) 2016/679.

ñ) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos que entrañe un alto riesgo para los derechos y libertades de los afectados, conforme a lo exigido por el artículo 34 del Reglamento (UE) 2016/679, salvo que resulte de aplicación lo previsto en el artículo 73 s) de esta ley orgánica.

o) Facilitar información inexacta a la Autoridad de protección de datos, en los supuestos en los que el responsable del tratamiento deba elevarle una consulta previa, conforme al artículo 36 del Reglamento (UE) 2016/679.

p) No publicar los datos de contacto del delegado de protección de datos, o no comunicarlos a la autoridad de protección de datos, cuando su nombramiento sea exigible de acuerdo con el artículo 37 del Reglamento (UE) 2016/679 y el artículo 34 de esta ley orgánica.

q) El incumplimiento por los organismos de certificación de la obligación de informar a la autoridad de protección de datos de la expedición, renovación o retirada de una certificación, conforme a lo exigido por los apartados 1 y 5 del artículo 43 del Reglamento (UE) 2016/679.

r) El incumplimiento por parte de los organismos acreditados de supervisión de un código de conducta de la obligación de informar a las autoridades de protección de datos acerca de las medidas que resulten oportunas en caso de infracción del código, conforme exige el artículo 41.4 del Reglamento (UE) 2016/679.

Artículo 75. *Interrupción de la prescripción de la infracción.*

Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del acuerdo de inicio.

Artículo 76. *Sanciones y medidas correctivas.*

1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.

3. Será posible, complementaria o alternativamente, la adopción, cuando proceda, de las restantes medidas correctivas a las que se refiere el artículo 83.2 del Reglamento (UE) 2016/679.
4. Será objeto de publicación en el Boletín Oficial del Estado la información que identifique al infractor, la infracción cometida y el importe de la sanción impuesta cuando la autoridad competente sea la Agencia Española de Protección de Datos, la sanción fuese superior a un millón de euros y el infractor sea una persona jurídica.
Cuando la autoridad competente para imponer la sanción sea una autoridad autonómica de protección de datos, se estará a su normativa de aplicación.

Artículo 77. *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento.*

1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.
b) Los órganos jurisdiccionales.
c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.
d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.
e) Las autoridades administrativas independientes.
f) El Banco de España.
g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.
h) Las fundaciones del sector público.
i) Las Universidades Públicas.
j) Los consorcios.
k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica.

Artículo 78. *Prescripción de las sanciones.*

1. Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 y de esta ley orgánica prescriben en los siguientes plazos:

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

TÍTULO X

Garantía de los derechos digitales

Artículo 79. *Los derechos en la Era digital.*

Los derechos y libertades consagrados en la Constitución y en los Tratados y Convenios Internacionales en que España sea parte son plenamente aplicables en Internet. Los prestadores de servicios de la sociedad de la información y los proveedores de servicios de Internet contribuirán a garantizar su aplicación.

Artículo 80. *Derecho a la neutralidad de Internet.*

Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos.

Artículo 81. *Derecho de acceso universal a Internet.*

1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica.

2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.

3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral.

4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores.

5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.

6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales.

Artículo 82. *Derecho a la seguridad digital.*

Los usuarios tienen derecho a la seguridad de las comunicaciones que transmitan y reciban a través de Internet. Los proveedores de servicios de Internet informarán a los usuarios de sus derechos.

Artículo 83. *Derecho a la educación digital.*

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un consumo responsable y un uso crítico y seguro de los medios digitales y respetuoso con la dignidad humana, la justicia social y la sostenibilidad medioambiental, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales.

Las Administraciones educativas deberán incluir en el desarrollo del currículo la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos en el apartado anterior.

3. Los planes de estudio de los títulos universitarios, en especial, aquellos que habiliten para el desempeño profesional en la formación del alumnado, garantizarán la formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.

4. Las Administraciones Públicas incorporarán a los temarios de las pruebas de acceso a los cuerpos superiores y a aquéllos en que habitualmente se desempeñen funciones que impliquen el acceso a datos personales materias relacionadas con la garantía de los derechos digitales y en particular el de protección de datos.

Artículo 84. *Protección de los menores en Internet.*

1. Los padres, madres, tutores, curadores o representantes legales procurarán que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de los servicios de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. La utilización o difusión de imágenes o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que puedan implicar una intromisión ilegítima en sus derechos fundamentales determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor.

Artículo 85. *Derecho de rectificación en Internet.*

1. Todos tienen derecho a la libertad de expresión en Internet.

2. Los responsables de redes sociales y servicios equivalentes adoptarán protocolos adecuados para posibilitar el ejercicio del derecho de rectificación ante los usuarios que difundan contenidos que atenten contra el derecho al honor, la intimidad personal y familiar en Internet y el derecho a comunicar o recibir libremente información veraz, atendiendo a los requisitos y procedimientos previstos en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

Cuando los medios de comunicación digitales deban atender la solicitud de rectificación formulada contra ellos deberán proceder a la publicación en sus archivos digitales de un aviso aclaratorio que ponga de manifiesto que la noticia original no refleja la situación actual del individuo. Dicho aviso deberá aparecer en lugar visible junto con la información original.

Artículo 86. *Derecho a la actualización de informaciones en medios de comunicación digitales.*

Toda persona tiene derecho a solicitar motivadamente de los medios de comunicación digitales la inclusión de un aviso de actualización suficientemente visible junto a las noticias que le conciernan cuando la información contenida en la noticia original no refleje su situación actual como consecuencia de circunstancias que hubieran tenido lugar después de la publicación, causándole un perjuicio.

En particular, procederá la inclusión de dicho aviso cuando las informaciones originales se refieran a actuaciones policiales o judiciales que se hayan visto afectadas en beneficio del interesado como consecuencia de decisiones judiciales posteriores. En este caso, el aviso hará referencia a la decisión posterior.

Artículo 87. *Derecho a la intimidad y uso de dispositivos digitales en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la protección de su intimidad en el uso de los dispositivos digitales puestos a su disposición por su empleador.

2. El empleador podrá acceder a los contenidos derivados del uso de medios digitales facilitados a los trabajadores a los solos efectos de controlar el cumplimiento de las obligaciones laborales o estatutarias y de garantizar la integridad de dichos dispositivos.

3. Los empleadores deberán establecer criterios de utilización de los dispositivos digitales respetando en todo caso los estándares mínimos de protección de su intimidad de acuerdo con los usos sociales y los derechos reconocidos constitucional y legalmente. En su elaboración deberán participar los representantes de los trabajadores.

El acceso por el empleador al contenido de dispositivos digitales respecto de los que haya admitido su uso con fines privados requerirá que se especifiquen de modo preciso los usos autorizados y se establezcan garantías para preservar la intimidad de los trabajadores, tales como, en su caso, la determinación de los períodos en que los dispositivos podrán utilizarse para fines privados.

Los trabajadores deberán ser informados de los criterios de utilización a los que se refiere este apartado.

Artículo 88. *Derecho a la desconexión digital en el ámbito laboral.*

1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar.

2. Las modalidades de ejercicio de este derecho atenderán a la naturaleza y objeto de la relación laboral, potenciarán el derecho a la conciliación de la actividad laboral y la vida personal y familiar y se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores.

3. El empleador, previa audiencia de los representantes de los trabajadores, elaborará una política interna dirigida a trabajadores, incluidos los que ocupen puestos directivos, en la que definirán las modalidades de ejercicio del derecho a la desconexión y las acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que evite el riesgo de fatiga informática. En particular, se preservará el derecho a la desconexión digital en los supuestos de realización total o parcial del trabajo a distancia

así como en el domicilio del empleado vinculado al uso con fines laborales de herramientas tecnológicas.

Artículo 89. *Derecho a la intimidad frente al uso de dispositivos de videovigilancia y de grabación de sonidos en el lugar de trabajo.*

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida.

En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el artículo 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en el apartado 3 del artículo 22 de esta ley.

Artículo 90. *Derecho a la intimidad ante la utilización de sistemas de geolocalización en el ámbito laboral.*

1. Los empleadores podrán tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el artículo 20.3 del Estatuto de los Trabajadores y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo.

2. Con carácter previo, los empleadores habrán de informar de forma expresa, clara e inequívoca a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de la existencia y características de estos dispositivos. Igualmente deberán informarles acerca del posible ejercicio de los derechos de acceso, rectificación, limitación del tratamiento y supresión.

Artículo 91. *Derechos digitales en la negociación colectiva.*

Los convenios colectivos podrán establecer garantías adicionales de los derechos y libertades relacionados con el tratamiento de los datos personales de los trabajadores y la salvaguarda de derechos digitales en el ámbito laboral.

Artículo 92. *Protección de datos de los menores en Internet.*

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad garantizarán la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.

Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes deberán contar con el consentimiento del menor o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

Artículo 93. *Derecho al olvido en búsquedas de Internet.*

1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet.

Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo.

2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho.

Artículo 94. *Derecho al olvido en servicios de redes sociales y servicios equivalentes.*

1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes.

2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información.

Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio.

Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas.

3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2.

Artículo 95. *Derecho de portabilidad en servicios de redes sociales y servicios equivalentes.*

Los usuarios de servicios de redes sociales y servicios de la sociedad de la información equivalentes tendrán derecho a recibir y transmitir los contenidos que hubieran facilitado a los prestadores de dichos servicios, así como a que los prestadores los transmitan directamente a otro prestador designado por el usuario, siempre que sea técnicamente posible.

Los prestadores podrán conservar, sin difundirla a través de Internet, copia de los contenidos cuando dicha conservación sea necesaria para el cumplimiento de una obligación legal.

Artículo 96. *Derecho al testamento digital.*

1. El acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas se regirá por las siguientes reglas:

a) Las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos podrán dirigirse a los prestadores de servicios de la sociedad de la información al

objeto de acceder a dichos contenidos e impartirles las instrucciones que estimen oportunas sobre su utilización, destino o supresión.

Como excepción, las personas mencionadas no podrán acceder a los contenidos del causante, ni solicitar su modificación o eliminación, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. Dicha prohibición no afectará al derecho de los herederos a acceder a los contenidos que pudiesen formar parte del caudal relicto.

b) El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los contenidos con vistas a dar cumplimiento a tales instrucciones.

c) En caso de personas fallecidas menores de edad, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada.

d) En caso de fallecimiento de personas con discapacidad, estas facultades podrán ejercerse también, además de por quienes señala la letra anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado.

2. Las personas legitimadas en el apartado anterior podrán decidir acerca del mantenimiento o eliminación de los perfiles personales de personas fallecidas en redes sociales o servicios equivalentes, a menos que el fallecido hubiera decidido acerca de esta circunstancia, en cuyo caso se estará a sus instrucciones.

El responsable del servicio al que se le comunique, con arreglo al párrafo anterior, la solicitud de eliminación del perfil, deberá proceder sin dilación a la misma.

3. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de los mandatos e instrucciones y, en su caso, el registro de los mismos, que podrá coincidir con el previsto en el artículo 3 de esta ley orgánica.

4. Lo establecido en este artículo en relación con las personas fallecidas en las comunidades autónomas con derecho civil, foral o especial, propio se regirá por lo establecido por estas dentro de su ámbito de aplicación.

Artículo 97. *Políticas de impulso de los derechos digitales.*

1. El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos:

a) superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, entre otras medidas, un bono social de acceso a Internet;

b) impulsar la existencia de espacios de conexión de acceso público; y

c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales.

2. Asimismo se aprobará un Plan de Actuación dirigido a promover las acciones de formación, difusión y concienciación necesarias para lograr que los menores de edad hagan un uso equilibrado y responsable de los dispositivos digitales y de las redes sociales y de los servicios de la sociedad de la información equivalentes de Internet con la finalidad de garantizar su adecuado desarrollo de la personalidad y de preservar su dignidad y derechos fundamentales.

3. El Gobierno presentará un informe anual ante la comisión parlamentaria correspondiente del Congreso de los Diputados en el que se dará cuenta de la evolución de los derechos, garantías y mandatos contemplados en el presente Título y de las medidas necesarias para promover su impulso y efectividad.

Disposición adicional primera. *Medidas de seguridad en el ámbito del sector público.*

1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.

2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad.

Disposición adicional segunda. *Protección de datos y transparencia y acceso a la información pública.*

La publicidad activa y el acceso a la información pública regulados por el Título I de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, así como las obligaciones de publicidad activa establecidas por la legislación autonómica, se someterán, cuando la información contenga datos personales, a lo dispuesto en los artículos 5.3 y 15 de la Ley 19/2013, en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición adicional tercera. *Cómputo de plazos.*

Los plazos establecidos en el Reglamento (UE) 2016/679 o en esta ley orgánica, con independencia de que se refieran a relaciones entre particulares o con entidades del sector público, se regirán por las siguientes reglas:

a) Cuando los plazos se señalen por días, se entiende que estos son hábiles, excluyéndose del cómputo los sábados, los domingos y los declarados festivos.

b) Si el plazo se fija en semanas, concluirá el mismo día de la semana en que se produjo el hecho que determina su iniciación en la semana de vencimiento.

c) Si el plazo se fija en meses o años, concluirá el mismo día en que se produjo el hecho que determina su iniciación en el mes o el año de vencimiento. Si en el mes de vencimiento no hubiera día equivalente a aquel en que comienza el cómputo, se entenderá que el plazo expira el último día del mes.

d) Cuando el último día del plazo sea inhábil, se entenderá prorrogado al primer día hábil siguiente.

Disposición adicional cuarta. *Procedimiento en relación con las competencias atribuidas a la Agencia Española de Protección de Datos por otras leyes.*

Lo dispuesto en el Título VIII y en sus normas de desarrollo será de aplicación a los procedimientos que la Agencia Española de Protección de Datos hubiera de tramitar en ejercicio de las competencias que le fueran atribuidas por otras leyes.

Disposición adicional quinta. *Autorización judicial en relación con decisiones de la Comisión Europea en materia de transferencia internacional de datos.*

1. Cuando una autoridad de protección de datos considerase que una decisión de la Comisión Europea en materia de transferencia internacional de datos, de cuya validez dependiese la resolución de un procedimiento concreto, infringiese lo dispuesto en el Reglamento (UE) 2016/679, menoscabando el derecho fundamental a la protección de datos, acordará inmediatamente la suspensión del procedimiento, a fin de solicitar del órgano judicial autorización para declararlo así en el seno del procedimiento del que esté conociendo. Dicha suspensión deberá ser confirmada, modificada o levantada en el acuerdo de admisión o inadmisión a trámite de la solicitud de la autoridad de protección de datos dirigida al tribunal competente.

Las decisiones de la Comisión Europea a las que puede resultar de aplicación este cauce son:

a) aquellas que declaren el nivel adecuado de protección de un tercer país u organización internacional, en virtud del artículo 45 del Reglamento (UE) 2016/679;

b) aquellas por las que se aprueben cláusulas tipo de protección de datos para la realización de transferencias internacionales de datos, o

c) aquellas que declaren la validez de los códigos de conducta a tal efecto.

2. La autorización a la que se refiere esta disposición solamente podrá ser concedida si, previo planteamiento de cuestión prejudicial de validez en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea, la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

Disposición adicional sexta. *Incorporación de deudas a sistemas de información crediticia.*

No se incorporarán a los sistemas de información crediticia a los que se refiere el artículo 20.1 de esta ley orgánica deudas en que la cuantía del principal sea inferior a cincuenta euros.

El Gobierno, mediante real decreto, podrá actualizar esta cuantía.

Disposición adicional séptima. *Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.*

1. Cuando sea necesaria la publicación de un acto administrativo que contuviese datos personales del afectado, se identificará al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

2. A fin de prevenir riesgos para víctimas de violencia de género, el Gobierno impulsará la elaboración de un protocolo de colaboración que defina procedimientos seguros de publicación y notificación de actos administrativos, con la participación de los órganos con competencia en la materia.

Disposición adicional octava. *Potestad de verificación de las Administraciones Públicas.*

Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos.

Disposición adicional novena. *Tratamiento de datos personales en relación con la notificación de incidentes de seguridad.*

Cuando, de conformidad con lo dispuesto en la legislación nacional que resulte de aplicación, deban notificarse incidentes de seguridad, las autoridades públicas competentes, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad, podrán tratar los datos personales contenidos en tales notificaciones, exclusivamente durante el tiempo y alcance necesarios para su análisis, detección, protección y respuesta ante

incidentes y adoptando las medidas de seguridad adecuadas y proporcionadas al nivel de riesgo determinado.

Disposición adicional décima. *Comunicaciones de datos por los sujetos enumerados en el artículo 77.1.*

Los responsables enumerados en el artículo 77.1 de esta ley orgánica podrán comunicar los datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento de los afectados o aprecien que concurre en los solicitantes un interés legítimo que prevalezca sobre los derechos e intereses de los afectados conforme a lo establecido en el artículo 6.1 f) del Reglamento (UE) 2016/679.

Disposición adicional undécima. *Privacidad en las comunicaciones electrónicas.*

Lo dispuesto en la presente ley orgánica se entenderá sin perjuicio de la aplicación de las normas de Derecho interno y de la Unión Europea reguladoras de la privacidad en el sector de las comunicaciones electrónicas, sin imponer obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación en ámbitos en los que estén sujetas a obligaciones específicas establecidas en dichas normas.

Disposición adicional duodécima. *Disposiciones específicas aplicables a los tratamientos de los registros de personal del sector público.*

1. Los tratamientos de los registros de personal del sector público se entenderán realizados en el ejercicio de poderes públicos conferidos a sus responsables, de acuerdo con lo previsto en el artículo 6.1.e) del Reglamento (UE) 2016/679.

2. Los registros de personal del sector público podrán tratar datos personales relativos a infracciones y condenas penales e infracciones y sanciones administrativas, limitándose a los datos estrictamente necesarios para el cumplimiento de sus fines.

3. De acuerdo con lo previsto en el artículo 18.2 del Reglamento (UE) 2016/679, y por considerarlo una razón de interés público importante, los datos cuyo tratamiento se haya limitado en virtud del artículo 18.1 del citado reglamento, podrán ser objeto de tratamiento cuando sea necesario para el desarrollo de los procedimientos de personal.

Disposición adicional decimotercera. *Transferencias internacionales de datos tributarios.*

Las transferencias de datos tributarios entre el Reino de España y otros Estados o entidades internacionales o supranacionales, se regularán por los términos y con los límites establecidos en la normativa sobre asistencia mutua entre los Estados de la Unión Europea, o en el marco de los convenios para evitar la doble imposición o de otros convenios internacionales, así como por las normas sobre la asistencia mutua establecidas en el Capítulo VI del Título III de la Ley 58/2003, de 17 de diciembre, General Tributaria.

Disposición adicional decimocuarta. *Normas dictadas en desarrollo del artículo 13 de la Directiva 95/46/CE.*

Las normas dictadas en aplicación del artículo 13 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que hubiesen entrado en vigor con anterioridad a 25 de mayo de 2018, y en particular los artículos 23 y 24 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, siguen vigentes en tanto no sean expresamente modificadas, sustituidas o derogadas.

Disposición adicional decimoquinta. *Requerimiento de información por parte de la Comisión Nacional del Mercado de Valores.*

Cuando no haya podido obtener por otros medios la información necesaria para realizar sus labores de supervisión e inspección relacionadas con la detección de delitos graves, la Comisión Nacional del Mercado de Valores podrá recabar de los operadores que presten

servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, los datos que obren en su poder relativos a la comunicación electrónica o servicio de la sociedad de la información proporcionados por dichos prestadores que sean distintos a su contenido y resulten imprescindibles para el ejercicio de dichas labores.

La cesión de estos datos requerirá la previa obtención de autorización judicial otorgada conforme a las normas procesales.

Disposición adicional decimosexta. *Prácticas agresivas en materia de protección de datos.*

A los efectos previstos en el artículo 8 de la Ley 3/1991, de 10 de enero, de Competencia Desleal, se consideran prácticas agresivas las siguientes:

a) Actuar con intención de suplantar la identidad de la Agencia Española de Protección de Datos o de una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos o a los interesados.

b) Generar la apariencia de que se está actuando en nombre, por cuenta o en colaboración con la Agencia Española de Protección de Datos o una autoridad autonómica de protección de datos en la realización de cualquier comunicación a los responsables y encargados de los tratamientos en que la remitente ofrezca sus productos o servicios.

c) Realizar prácticas comerciales en las que se coarte el poder de decisión de los destinatarios mediante la referencia a la posible imposición de sanciones por incumplimiento de la normativa de protección de datos personales.

d) Ofrecer cualquier tipo de documento por el que se pretenda crear una apariencia de cumplimiento de las disposiciones de protección de datos de forma complementaria a la realización de acciones formativas sin haber llevado a cabo las actuaciones necesarias para verificar que dicho cumplimiento se produce efectivamente.

e) Asumir, sin designación expresa del responsable o el encargado del tratamiento, la función de delegado de protección de datos y comunicarse en tal condición con la Agencia Española de Protección de Datos o las autoridades autonómicas de protección de datos.

Disposición adicional decimoséptima. *Tratamientos de datos de salud.*

1. Se encuentran amparados en las letras g), h), i) y j) del artículo 9.2 del Reglamento (UE) 2016/679 los tratamientos de datos relacionados con la salud y de datos genéticos que estén regulados en las siguientes leyes y sus disposiciones de desarrollo:

a) La Ley 14/1986, de 25 de abril, General de Sanidad.

b) La Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales.

c) La Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

d) La Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

e) La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias.

f) La Ley 14/2007, de 3 de julio, de Investigación biomédica.

g) La Ley 33/2011, de 4 de octubre, General de Salud Pública.

h) La Ley 20/2015, de 14 de julio, de ordenación, supervisión y solvencia de las entidades aseguradoras y reaseguradoras.

i) El texto refundido de la Ley de garantías y uso racional de los 105 medicamentos y productos sanitarios, aprobado por Real Decreto Legislativo 1/2015, de 24 de julio.

j) El texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado por Real Decreto Legislativo 1/2013 de 29 de noviembre.

2. El tratamiento de datos en la investigación en salud se regirá por los siguientes criterios:

a) El interesado o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora.

b) Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública.

c) Se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En tales casos, los responsables deberán publicar la información establecida por el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Para los tratamientos previstos en esta letra, se requerirá informe previo favorable del comité de ética de la investigación.

d) Se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica.

El uso de datos personales seudonimizados con fines de investigación en salud pública y biomédica requerirá:

1.º Una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación.

2.º Que los datos seudonimizados únicamente sean accesibles al equipo de investigación cuando:

i) Exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación.

ii) Se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados.

Podrá procederse a la reidentificación de los datos en su origen, cuando con motivo de una investigación que utilice datos seudonimizados, se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, o una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria.

e) Cuando se traten datos personales con fines de investigación en salud, y en particular la biomédica, a los efectos del artículo 89.2 del Reglamento (UE) 2016/679, podrán excepcionarse los derechos de los afectados previstos en los artículos 15, 16, 18 y 21 del Reglamento (EU) 2016/679 cuando:

1.º Los citados derechos se ejerzan directamente ante los investigadores o centros de investigación que utilicen datos anonimizados o seudonimizados.

2.º El ejercicio de tales derechos se refiera a los resultados de la investigación.

3.º La investigación tenga por objeto un interés público esencial relacionado con la seguridad del Estado, la defensa, la seguridad pública u otros objetivos importantes de interés público general, siempre que en este último caso la excepción esté expresamente recogida por una norma con rango de Ley.

f) Cuando conforme a lo previsto por el artículo 89 del Reglamento (UE) 2016/679, se lleve a cabo un tratamiento con fines de investigación en salud pública y, en particular, biomédica se procederá a:

1.º Realizar una evaluación de impacto que determine los riesgos derivados del tratamiento en los supuestos previstos en el artículo 35 del Reglamento (UE) 2016/679 o en los establecidos por la autoridad de control. Esta evaluación incluirá de modo específico los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos.

2.º Someter la investigación científica a las normas de calidad y, en su caso, a las directrices internacionales sobre buena práctica clínica.

3.º Adoptar, en su caso, medidas dirigidas a garantizar que los investigadores no acceden a datos de identificación de los interesados.

4.º Designar un representante legal establecido en la Unión Europea, conforme al artículo 74 del Reglamento (UE) 536/2014, si el promotor de un ensayo clínico no está establecido en la Unión Europea. Dicho representante legal podrá coincidir con el previsto en el artículo 27.1 del Reglamento (UE) 2016/679.

g) El uso de datos personales seudonimizados con fines de investigación en salud pública y, en particular, biomédica deberá ser sometido al informe previo del comité de ética de la investigación previsto en la normativa sectorial.

En defecto de la existencia del mencionado Comité, la entidad responsable de la investigación requerirá informe previo del delegado de protección de datos o, en su defecto, de un experto con los conocimientos previos en el artículo 37.5 del Reglamento (UE) 2016/679.

h) En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados.

Disposición adicional decimoctava. *Criterios de seguridad.*

La Agencia Española de Protección de Datos desarrollará, con la colaboración, cuando sea precisa, de todos los actores implicados, las herramientas, guías, directrices y orientaciones que resulten precisas para dotar a los profesionales, microempresas y pequeñas y medianas empresas de pautas adecuadas para el cumplimiento de las obligaciones de responsabilidad activa establecidas en el Título IV del Reglamento (UE) 2016/679 y en el Título V de esta ley orgánica.

Disposición adicional decimonovena. *Derechos de los menores ante Internet.*

En el plazo de un año desde la entrada en vigor de esta ley orgánica, el Gobierno remitirá al Congreso de los Diputados un proyecto de ley dirigido específicamente a garantizar los derechos de los menores ante el impacto de Internet, con el fin de garantizar su seguridad y luchar contra la discriminación y la violencia que sobre los mismos es ejercida mediante las nuevas tecnologías.

Disposición adicional vigésima. *Especialidades del régimen jurídico de la Agencia Española de Protección de Datos.*

1. No será de aplicación a la Agencia Española de Protección de Datos el artículo 50.2.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. La Agencia Española de Protección de Datos podrá adherirse a los sistemas de contratación centralizada establecidos por las Administraciones Públicas y participar en la gestión compartida de servicios comunes prevista en el artículo 85 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Disposición adicional vigésima primera. *Educación digital.*

Las Administraciones educativas darán cumplimiento al mandato contenido en el párrafo segundo del apartado 1 del artículo 83 de esta ley orgánica en el plazo de un año a contar desde la entrada en vigor de la misma.

Disposición adicional vigésima segunda. *Acceso a los archivos públicos y eclesiásticos.*

Las autoridades públicas competentes facilitarán el acceso a los archivos públicos y eclesiásticos en relación con los datos que se soliciten con ocasión de investigaciones policiales o judiciales de personas desaparecidas, debiendo atender las solicitudes con prontitud y diligencia las instituciones o congregaciones religiosas a las que se realicen las peticiones de acceso.

Disposición adicional vigésima tercera. *Modelos de presentación de reclamaciones.*

La Agencia Española de Protección de Datos podrá establecer modelos de presentación de reclamaciones ante la misma en todos los ámbitos en los que ésta tenga competencia, que serán de uso obligatorio para los interesados independientemente de que estén obligados o no a relacionarse electrónicamente con las administraciones públicas.

Los modelos serán publicados en el "Boletín Oficial del Estado" y en la Sede Electrónica de la Agencia Española de Protección de Datos y serán de obligado cumplimiento al mes de su publicación en el "Boletín Oficial del Estado".»

Disposición transitoria primera. *Estatuto de la Agencia Española de Protección de Datos.*

1. El Estatuto de la Agencia Española de Protección de Datos, aprobado por Real Decreto 428/1993, de 26 de marzo, continuará vigente en lo que no se oponga a lo establecido en el Título VIII de esta ley orgánica.

2. Lo dispuesto en los apartados 2, 3 y 5 del artículo 48 y en el artículo 49 de esta ley orgánica se aplicará una vez expire el mandato de quien ostente la condición de Director de la Agencia Española de Protección de Datos a la entrada en vigor de la misma.

Disposición transitoria segunda. *Códigos tipo inscritos en las autoridades de protección de datos conforme a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

Los promotores de los códigos tipo inscritos en el registro de la Agencia Española de Protección de Datos o en las autoridades autonómicas de protección de datos deberán adaptar su contenido a lo dispuesto en el artículo 40 del Reglamento (UE) 2016/679 en el plazo de un año a contar desde la entrada en vigor de esta ley orgánica.

Si, transcurrido dicho plazo, no se hubiera solicitado la aprobación prevista en el artículo 38.4 de esta ley orgánica, se cancelará la inscripción y se comunicará a sus promotores.

Disposición transitoria tercera. *Régimen transitorio de los procedimientos.*

1. Los procedimientos ya iniciados a la entrada en vigor de esta ley orgánica se regirán por la normativa anterior, salvo que esta ley orgánica contenga disposiciones más favorables para el interesado.

2. Lo dispuesto en el apartado anterior será asimismo de aplicación a los procedimientos respecto de los cuales ya se hubieren iniciado las actuaciones previas a las que se refiere la Sección 2.ª del Capítulo III del Título IX del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre.

Disposición transitoria cuarta. *Tratamientos sometidos a la Directiva (UE) 2016/680.*

Los tratamientos sometidos a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, continuarán rigiéndose por la Ley Orgánica 15/1999, de 13 de diciembre, y en particular el artículo 22, y sus disposiciones de desarrollo, en tanto no entre en vigor la norma que trasponga al Derecho español lo dispuesto en la citada directiva.

Téngase en cuenta que la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, ha sido transpuesta por la Ley Orgánica 7/2021, de 26 de mayo. Ref. BOE-A-2021-8806

Disposición transitoria quinta. *Contratos de encargado del tratamiento.*

Los contratos de encargado del tratamiento suscritos con anterioridad al 25 de mayo de 2018 al amparo de lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y en caso de haberse pactado de forma indefinida, hasta el 25 de mayo de 2022.

Durante dichos plazos cualquiera de las partes podrá exigir a la otra la modificación del contrato a fin de que el mismo resulte conforme a lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679 y en el Capítulo II del Título V de esta ley orgánica.

Disposición transitoria sexta. *Reutilización con fines de investigación en materia de salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de esta ley orgánica.*

Se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos lícitamente con anterioridad a la entrada en vigor de esta ley orgánica cuando concurra alguna de las circunstancias siguientes:

a) Que dichos datos personales se utilicen para la finalidad concreta para la que se hubiera prestado consentimiento.

b) Que, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen tales datos para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

Disposición derogatoria única. *Derogación normativa.*

1. Sin perjuicio de lo previsto en la disposición adicional decimocuarta y en la disposición transitoria cuarta, queda derogada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. Queda derogado el Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos.

3. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango contradigan, se opongan, o resulten incompatibles con lo dispuesto en el Reglamento (UE) 2016/679 y en la presente ley orgánica.

Disposición final primera. *Naturaleza de la presente ley.*

La presente ley tiene el carácter de ley orgánica.

No obstante, tienen carácter de ley ordinaria:

– El Título IV,
– el Título VII, salvo los artículos 52 y 53, que tienen carácter orgánico,
– el Título VIII,
– el Título IX,
– los artículos 79, 80, 81, 82, 88, 95, 96 y 97 del Título X,
– las disposiciones adicionales, salvo la disposición adicional segunda y la disposición adicional decimoséptima, que tienen carácter orgánico,
– las disposiciones transitorias,
– y las disposiciones finales, salvo las disposiciones finales primera, segunda, tercera, cuarta, octava, décima y decimosexta, que tienen carácter orgánico.

Disposición final segunda. *Título competencial.*

1. Esta ley orgánica se dicta al amparo del artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

2. El Capítulo I del Título VII, el Título VIII, la disposición adicional cuarta y la disposición transitoria primera sólo serán de aplicación a la Administración General del Estado y a sus organismos públicos.

3. Los artículos 87 a 90 se dictan al amparo de la competencia exclusiva que el artículo 149.1.7.ª y 18.ª de la Constitución reserva al Estado en materia de legislación laboral y bases del régimen estatutario de los funcionarios públicos respectivamente.

4. La disposición adicional quinta y las disposiciones finales séptima y sexta se dictan al amparo de la competencia que el artículo 149.1.6.ª de la Constitución atribuye al Estado en materia de legislación procesal.

5. La disposición adicional tercera se dicta al amparo del artículo 149.1.18.ª de la Constitución.

6. El artículo 96 se dicta al amparo del artículo 149.1.8.ª de la Constitución.

Disposición final tercera. *Modificación de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General.*

Se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General que queda redactada como sigue:

Uno. El apartado 3 del artículo treinta y nueve queda redactado como sigue:

> «3. Dentro del plazo anterior, cualquier persona podrá formular reclamación dirigida a la Delegación Provincial de la Oficina del Censo Electoral sobre sus datos censales, si bien solo podrán ser tenidas en cuenta las que se refieran a la rectificación de errores en los datos personales, a los cambios de domicilio dentro de una misma circunscripción o a la no inclusión del reclamante en ninguna Sección del Censo de la circunscripción pese a tener derecho a ello. También serán atendidas las solicitudes de los electores que se opongan a su inclusión en las copias del censo electoral que se faciliten a los representantes de las candidaturas para realizar envíos postales de propaganda electoral. No serán tenidas en cuenta para la elección convocada las que reflejen un cambio de residencia de una circunscripción a otra, realizado con posterioridad a la fecha de cierre del censo para cada elección, debiendo ejercer su derecho en la sección correspondiente a su domicilio anterior.»

Dos. Se añade un nuevo artículo cincuenta y ocho bis, con el contenido siguiente:

> **«Artículo cincuenta y ocho bis.** *Utilización de medios tecnológicos y datos personales en las actividades electorales.*
>
> 1. **(Anulado)**
>
> 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.
>
> 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.
>
> 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.
>
> 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.»

Disposición final cuarta. *Modificación de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.*

Se modifica la Ley Orgánica, 6/1985, de 1 de julio, del Poder Judicial, en los siguientes términos:

Uno. Se añade un apartado tercero al artículo 58, con la siguiente redacción:

«Artículo 58.

Tercero. De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por el Consejo General del Poder Judicial.»

Dos. Se añade una letra f) al artículo 66, con la siguiente redacción:

«Artículo 66.

f) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añaden una letra k) al apartado 1 y un nuevo apartado 7 al artículo 74, con la siguiente redacción:

«Artículo 74.

1. […]

k) De la solicitud de autorización para la declaración prevista en la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando tal solicitud sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.

[…]

7. Corresponde a las Salas de lo Contencioso-administrativo de los Tribunales Superiores de Justicia autorizar, mediante auto, el requerimiento de información por parte de autoridades autonómicas de protección de datos a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Cuatro. Se añade un nuevo apartado 7 al artículo 90:

«7. Corresponde a los Juzgados Centrales de lo Contencioso-administrativo autorizar, mediante auto, el requerimiento de información por parte de la Agencia Española de Protección de Datos y otras autoridades administrativas independientes de ámbito estatal a los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información, cuando ello sea necesario de acuerdo con la legislación específica.»

Disposición final quinta. *Modificación de la Ley 14/1986, de 25 de abril, General de Sanidad.*

Se añade un nuevo Capítulo II al Título VI de la Ley 14/1986, de 25 de abril, General de Sanidad con el siguiente contenido:

«CAPÍTULO II

Tratamiento de datos de la investigación en salud

Artículo 105 bis.

El tratamiento de datos personales en la investigación en salud se regirá por lo dispuesto en la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.»

Disposición final sexta. *Modificación de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.*

La Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, se modifica en los siguientes términos:

Uno. Se añade un nuevo apartado 7 al artículo 10:

«7. Conocerán de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la autoridad de protección de datos de la Comunidad Autónoma respectiva.»

Dos. Se añade un nuevo apartado 5 al artículo 11:

«5. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por la Agencia Española de Protección de Datos.»

Tres. Se añade un nuevo apartado 4 al artículo 12:

«4. Conocerá de la solicitud de autorización al amparo del artículo 122 ter, cuando sea formulada por el Consejo General del Poder Judicial.»

Cuatro. Se introduce un nuevo artículo 122 ter, con el siguiente tenor:

«Artículo 122 ter. *Procedimiento de autorización judicial de conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos.*

1. El procedimiento para obtener la autorización judicial a que se refiere la disposición adicional quinta de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, se iniciará con la solicitud de la autoridad de protección de datos dirigida al Tribunal competente para que se pronuncie acerca de la conformidad de una decisión de la Comisión Europea en materia de transferencia internacional de datos con el Derecho de la Unión Europea. La solicitud irá acompañada de copia del expediente que se encontrase pendiente de resolución ante la autoridad de protección de datos.

2. Serán partes en el procedimiento, además de la autoridad de protección de datos, quienes lo fueran en el procedimiento tramitado ante ella y, en todo caso, la Comisión Europea.

3. El acuerdo de admisión o inadmisión a trámite del procedimiento confirmará, modificará o levantará la suspensión del procedimiento por posible vulneración de la normativa de protección de datos tramitado ante la autoridad de protección de datos, del que trae causa este procedimiento de autorización judicial.

4. Admitida a trámite la solicitud, el Tribunal competente lo notificará a la autoridad de protección de datos a fin de que dé traslado a quienes interviniesen en el procedimiento tramitado ante la misma para que se personen en el plazo de tres días. Igualmente, se dará traslado a la Comisión Europea a los mismos efectos.

5. Concluido el plazo mencionado en la letra anterior, se dará traslado de la solicitud de autorización a las partes personadas a fin de que en el plazo de diez días aleguen lo que estimen procedente, pudiendo solicitar en ese momento la práctica de las pruebas que estimen necesarias.

6. Transcurrido el período de prueba, si alguna de las partes lo hubiese solicitado y el órgano jurisdiccional lo estimase pertinente, se celebrará una vista. El Tribunal

podrá decidir el alcance de las cuestiones sobre las que las partes deberán centrar sus alegaciones en dicha vista.

7. Finalizados los trámites mencionados en los tres apartados anteriores, el Tribunal competente adoptará en el plazo de diez días una de estas decisiones:

a) Si considerase que la decisión de la Comisión Europea es conforme al Derecho de la Unión Europea, dictará sentencia declarándolo así y denegando la autorización solicitada.

b) En caso de considerar que la decisión es contraria al Derecho de la Unión Europea, dictará auto de planteamiento de cuestión prejudicial de validez de la citada decisión ante el Tribunal de Justicia de la Unión Europea, en los términos del artículo 267 del Tratado de Funcionamiento de la Unión Europea.

La autorización solamente podrá ser concedida si la decisión de la Comisión Europea cuestionada fuera declarada inválida por el Tribunal de Justicia de la Unión Europea.

8. El régimen de recursos será el previsto en esta ley.»

Disposición final séptima. *Modificación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.*

Se modifica el artículo 15 bis de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, que queda redactado como sigue:

«Artículo 15 bis. *Intervención en procesos de defensa de la competencia y de protección de datos.*

1. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas en el ámbito de sus competencias podrán intervenir en los procesos de defensa de la competencia y de protección de datos, sin tener la condición de parte, por propia iniciativa o a instancia del órgano judicial, mediante la aportación de información o presentación de observaciones escritas sobre cuestiones relativas a la aplicación de los artículos 101 y 102 del Tratado de Funcionamiento de la Unión Europea o los artículos 1 y 2 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Con la venia del correspondiente órgano judicial, podrán presentar también observaciones verbales. A estos efectos, podrán solicitar al órgano jurisdiccional competente que les remita o haga remitir todos los documentos necesarios para realizar una valoración del asunto de que se trate.

La aportación de información no alcanzará a los datos o documentos obtenidos en el ámbito de las circunstancias de aplicación de la exención o reducción del importe de las multas previstas en los artículos 65 y 66 de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia.

2. La Comisión Europea, la Comisión Nacional de los Mercados y la Competencia y los órganos competentes de las comunidades autónomas aportarán la información o presentarán las observaciones previstas en el número anterior diez días antes de la celebración del acto del juicio a que se refiere el artículo 433 o dentro del plazo de oposición o impugnación del recurso interpuesto.

3. Lo dispuesto en los anteriores apartados en materia de procedimiento será asimismo de aplicación cuando la Comisión Europea, la Agencia Española de Protección de Datos y las autoridades autonómicas de protección de datos, en el ámbito de sus competencias, consideren precisa su intervención en un proceso que afecte a cuestiones relativas a la aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.»

Disposición final octava. *Modificación de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.*

Se incluye una nueva letra l) en el apartado 2 del artículo 46 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, con el contenido siguiente:

«l) La formación en el uso y seguridad de los medios digitales y en la garantía de los derechos fundamentales en Internet.»

Disposición final novena. *Modificación de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.*

Se modifica el apartado 3 del artículo 16 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, que pasa a tener el siguiente tenor:

«Artículo 16. *[…]*

3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clinicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

Asimismo se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clinicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.

Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.»

Disposición final décima. *Modificación de la Ley Orgánica 2/2006, de 3 de mayo, de Educación.*

Se incluye una nueva letra l) en el apartado 1 del artículo 2 de la Ley Orgánica 2/2006, de 3 de mayo, de Educación, que queda redactado como sigue:

«l) La capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva.»

Disposición final undécima. *Modificación de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.*

Se modifica la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en los siguientes términos:

Uno. Se añade un nuevo artículo 6 bis, con la siguiente redacción:

«Artículo 6 bis. *Registro de actividades de tratamiento.*

Los sujetos enumerados en el artículo 77.1 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, publicarán su inventario de actividades de tratamiento en aplicación del artículo 31 de la citada Ley Orgánica.»

Dos. El apartado 1 del artículo 15 queda redactado como sigue:

«1. Si la información solicitada contuviera datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso.

Si la información incluyese datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluyese datos genéticos o biométricos o contuviera datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley.»

Disposición final duodécima. *Modificación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.*

Se modifican los apartados 2 y 3 del artículo 28 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que pasan a tener la siguiente redacción:

«Artículo 28. *[…]*

2. Los interesados tienen derecho a no aportar documentos que ya se encuentren en poder de la Administración actuante o hayan sido elaborados por cualquier otra Administración. La administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello. No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección.

Las Administraciones Públicas deberán recabar los documentos electrónicamente a través de sus redes corporativas o mediante consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto.

Cuando se trate de informes preceptivos ya elaborados por un órgano administrativo distinto al que tramita el procedimiento, estos deberán ser remitidos en el plazo de diez días a contar desde su solicitud. Cumplido este plazo, se informará al interesado de que puede aportar este informe o esperar a su remisión por el órgano competente.

3. Las Administraciones no exigirán a los interesados la presentación de documentos originales, salvo que, con carácter excepcional, la normativa reguladora aplicable establezca lo contrario.

Asimismo, las Administraciones Públicas no requerirán a los interesados datos o documentos no exigidos por la normativa reguladora aplicable o que hayan sido aportados anteriormente por el interesado a cualquier Administración. A estos efectos, el interesado deberá indicar en qué momento y ante qué órgano administrativo presentó los citados documentos, debiendo las Administraciones Públicas recabarlos electrónicamente a través de sus redes corporativas o de una consulta a las plataformas de intermediación de datos u otros sistemas electrónicos habilitados al efecto, salvo que conste en el procedimiento la oposición expresa del interesado o la ley especial aplicable requiera su consentimiento expreso. Excepcionalmente, si las Administraciones Públicas no pudieran recabar los citados documentos, podrán solicitar nuevamente al interesado su aportación.»

Disposición final decimotercera. *Modificación del texto refundido de la Ley del Estatuto de los Trabajadores.*

Se añade un nuevo artículo 20 bis al texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 2/2015, de 23 de octubre, con el siguiente contenido:

> **«Artículo 20 bis.** *Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión.*
>
> Los trabajadores tienen derecho a la intimidad en el uso de los dispositivos digitales puestos a su disposición por el empleador, a la desconexión digital y a la intimidad frente al uso de dispositivos de videovigilancia y geolocalización en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimocuarta. *Modificación del texto refundido de la Ley del Estatuto Básico del Empleado Público.*

Se añade una nueva letra j bis) en el artículo 14 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, que quedará redactada como sigue:

> «j bis) A la intimidad en el uso de dispositivos digitales puestos a su disposición y frente al uso de dispositivos de videovigilancia y geolocalización, así como a la desconexión digital en los términos establecidos en la legislación vigente en materia de protección de datos personales y garantía de los derechos digitales.»

Disposición final decimoquinta. *Desarrollo normativo.*

Se habilita al Gobierno para desarrollar lo dispuesto en los artículos 3.2, 38.6, 45.2, 63.3, 96.3 y disposición adicional sexta, en los términos establecidos en ellos.

Disposición final decimosexta. *Entrada en vigor.*

La presente ley orgánica entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

§ 63

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Ministerio de Justicia
«BOE» núm. 17, de 19 de enero de 2008
Última modificación: 8 de marzo de 2012
Referencia: BOE-A-2008-979

La actual Ley Orgánica 15/1999, de 13 de diciembre de Protección de datos de carácter personal adaptó nuestro ordenamiento a lo dispuesto por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, derogando a su vez la hasta entonces vigente Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de datos de carácter personal.

La nueva ley, que ha nacido con una amplia vocación de generalidad, prevé en su artículo 1 que «tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal». Comprende por tanto el tratamiento automatizado y el no automatizado de los datos de carácter personal.

A fin de garantizar la necesaria seguridad jurídica en un ámbito tan sensible para los derechos fundamentales como el de la protección de datos, el legislador declaró subsistentes las normas reglamentarias existentes y, en especial, los reales decretos 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos, 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre de Regulación del tratamiento automatizado de los datos de carácter personal y 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, a la vez que habilitó al Gobierno para la aprobación o modificación de las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la Ley Orgánica 15/1999.

Por otra parte, la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones atribuyen competencias en materia sancionadora a la Agencia Española de Protección de Datos. Éstas requieren de desarrollo reglamentario con la peculiaridad de que ambas normas se ordenan a la tutela no sólo de los derechos de las personas físicas, sino también de las jurídicas.

II

Este Reglamento comparte con la Ley Orgánica la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales. Por ello, ha de destacarse que esta norma reglamentaria nace con la vocación de no reiterar los contenidos de la norma superior y de desarrollar, no sólo los mandatos contenidos en la Ley Orgánica de acuerdo con los principios que emanan de la Directiva, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

Por tanto, se aprueba este Reglamento partiendo de la necesidad de dotar de coherencia a la regulación reglamentaria en todo lo relacionado con la transposición de la Directiva y de desarrollar los aspectos novedosos de la Ley Orgánica 15/1999, junto con aquellos en los que la experiencia ha aconsejado un cierto de grado de precisión que dote de seguridad jurídica al sistema.

III

El reglamento viene a abarcar el ámbito tutelado anteriormente por los reales decretos 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia.

El título I contempla el objeto y ámbito de aplicación del reglamento. A lo largo de la vigencia de la Ley Orgánica 15/1999, se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Por otra parte, el presente reglamento no contiene previsiones para los tratamientos de datos personales a los que se refiere el apartado 3 del artículo 2 de la ley orgánica, dado que se rigen por sus disposiciones específicas y por lo especialmente previsto, en su caso, por la propia Ley Orgánica 15/1999. En consecuencia, se mantiene el régimen jurídico propio de estos tratamientos y ficheros.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Asimismo, se ofrece lo que no puede definirse sino como un estatuto del encargado del tratamiento, que sin duda contribuirá a clarificar todo lo relacionado con esta figura. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, según ha afirmado el Tribunal Constitucional en su sentencia número 292/2000, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial-, el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, finalmente, la regulación de un instrumento, el código tipo, llamado a jugar cada vez un papel más relevante como elemento dinamizador del derecho fundamental a la protección de datos.

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales. La repercusión del deber de seguridad obligaba a un particular rigor ya que en esta materia han confluido distintos elementos muy relevantes. Por una parte, la experiencia dimanante de la aplicación del Real Decreto 994/1999 permitía conocer las dificultades que habían enfrentado los responsables e identificar los puntos débiles y fuertes de la regulación. Por otra, se reclamaba la adaptación de la regulación en distintos aspectos. En este sentido, el reglamento trata de ser particularmente riguroso en la atribución de los niveles de seguridad, en la fijación de las medidas que corresponda adoptar en cada caso y en la revisión de las mismas cuando ello resulte necesario. Por otra parte, ordena con mayor precisión el contenido y las obligaciones vinculadas al mantenimiento del documento de seguridad. Además, se ha pretendido regular la materia de modo que contemple las múltiples formas de organización material y personal de la seguridad que se dan en la práctica. Por último, se regula un conjunto de medidas destinadas a los ficheros y tratamientos estructurados y no automatizados que ofrezca a los responsables un marco claro de actuación.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se ha optado por normar exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al presente reglamento.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa de la Ministra de Administraciones Públicas, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 21 de diciembre de 2007.

D I S P O N G O :

Artículo único. *Aprobación del reglamento.*

Se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, cuyo texto se incluye a continuación.

Disposición transitoria primera. *Adaptación de los códigos tipo inscritos en el Registro General de Protección de Datos.*

En el plazo de un año desde la entrada en vigor del presente real decreto deberán notificarse a la Agencia Española de Protección de Datos las modificaciones que resulten necesarias en los códigos tipo inscritos en el Registro General de Protección de Datos para adaptar su contenido a lo dispuesto en el título VII del mismo.

Disposición transitoria segunda. *Plazos de implantación de las medidas de seguridad.*

La implantación de las medidas de seguridad previstas en el presente real decreto deberá producirse con arreglo a las siguientes reglas:

1.ª Respecto de los ficheros automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) En el plazo de un año desde su entrada en vigor, deberán implantarse las medidas de seguridad de nivel medio exigibles a los siguientes ficheros:

1.º Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias.

2.º Aquéllos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

3.º Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos, respecto de las medidas de este nivel que no fueran exigibles conforme a lo previsto en el artículo 4.4 del Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio.

b) En el plazo de un año desde su entrada en vigor deberán implantarse las medidas de seguridad de nivel medio y en el de dieciocho meses desde aquella fecha, las de nivel alto exigibles a los siguientes ficheros:

1.º Aquéllos que contengan datos derivados de actos de violencia de género.

2.º Aquéllos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización.

c) En los demás supuestos, cuando el presente reglamento exija la implantación de una medida adicional, no prevista en el Reglamento de Medidas de seguridad de los ficheros automatizados de datos de carácter personal, aprobado por Real Decreto 994/1999, de 11 de junio, dicha medida deberá implantarse en el plazo de un año desde la entrada en vigor del presente real decreto.

2.ª Respecto de los ficheros no automatizados que existieran en la fecha de entrada en vigor del presente real decreto:

a) Las medidas de seguridad de nivel básico deberán implantarse en el plazo de un año desde su entrada en vigor.

b) Las medidas de seguridad de nivel medio deberán implantarse en el plazo de dieciocho meses desde su entrada en vigor.

c) Las medidas de seguridad de nivel alto deberán implantarse en el plazo de dos años desde su entrada en vigor.

3.ª Los ficheros, tanto automatizados como no automatizados, creados con posterioridad a la fecha de entrada en vigor del presente real decreto deberán tener implantadas, desde el momento de su creación la totalidad de las medidas de seguridad reguladas en el mismo.

Disposición transitoria tercera. *Régimen transitorio de las solicitudes para el ejercicio de los derechos de las personas.*

A las solicitudes para el ejercicio de los derechos de acceso, oposición, rectificación y cancelación que hayan sido efectuadas antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria cuarta. *Régimen transitorio de los procedimientos.*

A los procedimientos ya iniciados antes de la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

Disposición transitoria quinta. *Régimen transitorio de las actuaciones previas.*

A las actuaciones previas iniciadas con anterioridad a la entrada en vigor del presente real decreto, no les será de aplicación el mismo, rigiéndose por la normativa anterior.

El presente real decreto se aplicará a las actuaciones previas que se inicien después de su entrada en vigor.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogados el Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del

tratamiento automatizado de los datos de carácter personal, el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal y todas las normas de igual o inferior rango que contradigan o se opongan a lo dispuesto en el presente real decreto.

Disposición final primera. *Título competencial.*

El título I, con excepción del apartado c) del artículo 4, los títulos II, III, VII y VIII, así como los artículos 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 y 63.3 del reglamento se dictan al amparo de lo dispuesto en el artículo 149.1.1.ª de la Constitución, que atribuye al Estado la competencia exclusiva para la regulación de las condiciones básicas que garanticen la igualdad de todos los españoles en el ejercicio de los derechos y en el cumplimiento de los deberes constitucionales.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor a los tres meses de su íntegra publicación en el «Boletín Oficial del Estado».

REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA 15/1999, DE 13 DE DICIEMBRE, DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente reglamento tiene por objeto el desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal.

2. Asimismo, el capítulo III del título IX de este reglamento desarrolla las disposiciones relativas al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora, en aplicación de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, en el título VII de la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en el título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 2. *Ámbito objetivo de aplicación.*

1. El presente reglamento será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales.

3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal.

4. Este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

Artículo 3. *Ámbito territorial de aplicación.*

1. Se regirá por el presente reglamento todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento, siempre que dicho establecimiento se encuentre ubicado en territorio español.

Cuando no resulte de aplicación lo dispuesto en el párrafo anterior, pero exista un encargado del tratamiento ubicado en España, serán de aplicación al mismo las normas contenidas en el título VIII del presente reglamento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española, según las normas de Derecho internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En este supuesto, el responsable del tratamiento deberá designar un representante establecido en territorio español.

2. A los efectos previstos en los apartados anteriores, se entenderá por establecimiento, con independencia de su forma jurídica, cualquier instalación estable que permita el ejercicio efectivo y real de una actividad.

Artículo 4. *Ficheros o tratamientos excluidos.*

El régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos:

a) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares.

b) A los sometidos a la normativa sobre protección de materias clasificadas.

c) A los establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

Artículo 5. *Definiciones.*

1. A los efectos previstos en este reglamento, se entenderá por:

a) Afectado o interesado: Persona física titular de los datos que sean objeto del tratamiento.

b) Cancelación: Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

c) Cesión o comunicación de datos: Tratamiento de datos que supone su revelación a una persona distinta del interesado.

d) Consentimiento del interesado: Toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

e) Dato disociado: aquél que no permite la identificación de un afectado o interesado.

f) Datos de carácter personal: Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

g) Datos de carácter personal relacionados con la salud: las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.

h) Destinatario o cesionario: la persona física o jurídica, pública o privada u órgano administrativo, al que se revelen los datos.

Podrán ser también destinatarios los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

i) Encargado del tratamiento: La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

j) Exportador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero.

k) Fichero: Todo conjunto organizado de datos de carácter personal, que permita el acceso a los datos con arreglo a criterios determinados, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

l) Ficheros de titularidad privada: los ficheros de los que sean responsables las personas, empresas o entidades de derecho privado, con independencia de quien ostente la titularidad de su capital o de la procedencia de sus recursos económicos, así como los ficheros de los que sean responsables las corporaciones de derecho público, en cuanto dichos ficheros no se encuentren estrictamente vinculados al ejercicio de potestades de derecho público que a las mismas atribuye su normativa específica.

m) Ficheros de titularidad pública: los ficheros de los que sean responsables los órganos constitucionales o con relevancia constitucional del Estado o las instituciones autonómicas con funciones análogas a los mismos, las Administraciones públicas territoriales, así como las entidades u organismos vinculados o dependientes de las mismas y las Corporaciones de derecho público siempre que su finalidad sea el ejercicio de potestades de derecho público.

n) Fichero no automatizado: todo conjunto de datos de carácter personal organizado de forma no automatizada y estructurado conforme a criterios específicos relativos a personas físicas, que permitan acceder sin esfuerzos desproporcionados a sus datos personales, ya sea aquél centralizado, descentralizado o repartido de forma funcional o geográfica.

ñ) Importador de datos personales: la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero.

o) Persona identificable: toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados.

p) Procedimiento de disociación: Todo tratamiento de datos personales que permita la obtención de datos disociados.

q) Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

r) Tercero: la persona física o jurídica, pública o privada u órgano administrativo distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento.

Podrán ser también terceros los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

s) Transferencia internacional de datos: Tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien

constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español.

t) Tratamiento de datos: cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

2. En particular, en relación con lo dispuesto en el título VIII de este reglamento se entenderá por:

a) Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

b) Autenticación: procedimiento de comprobación de la identidad de un usuario.

c) Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario o en el acceso a un recurso.

d) Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

e) Copia de respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

f) Documento: todo escrito, gráfico, sonido, imagen o cualquier otra clase de información que puede ser tratada en un sistema de información como una unidad diferenciada.

g) Ficheros temporales: ficheros de trabajo creados por usuarios o procesos que son necesarios para un tratamiento ocasional o como paso intermedio durante la realización de un tratamiento.

h) Identificación: procedimiento de reconocimiento de la identidad de un usuario.

i) Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

j) Perfil de usuario: accesos autorizados a un grupo de usuarios.

k) Recurso: cualquier parte componente de un sistema de información.

l) Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

m) Sistema de información: conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

n) Sistema de tratamiento: modo en que se organiza o utiliza un sistema de información. Atendiendo al sistema de tratamiento, los sistemas de información podrán ser automatizados, no automatizados o parcialmente automatizados.

ñ) Soporte: objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos.

o) Transmisión de documentos: cualquier traslado, comunicación, envío, entrega o divulgación de la información contenida en el mismo.

p) Usuario: sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

Artículo 6. *Cómputo de plazos.*

En los supuestos en que este reglamento señale un plazo por días se computarán únicamente los hábiles. Cuando el plazo sea por meses, se computarán de fecha a fecha.

Artículo 7. *Fuentes accesibles al público.*

1. A efectos del artículo 3, párrafo j) de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público:

a) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

b) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica.

c) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional.

d) Los diarios y boletines oficiales.

e) Los medios de comunicación social.

2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

TÍTULO II

Principios de protección de datos

CAPÍTULO I

Calidad de los datos

Artículo 8. *Principios relativos a la calidad de los datos.*

1. Los datos de carácter personal deberán ser tratados de forma leal y lícita. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

2. Los datos de carácter personal sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento.

3. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos.

4. Sólo podrán ser objeto de tratamiento los datos que sean adecuados, pertinentes y no excesivos en relación con las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

5. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado. Si los datos fueran recogidos directamente del afectado, se considerarán exactos los facilitados por éste.

Si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud, salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello.

Cuando los datos hubieran sido comunicados previamente, el responsable del fichero o tratamiento deberá notificar al cesionario, en el plazo de diez días, la rectificación o cancelación efectuada, siempre que el cesionario sea conocido.

En el plazo de diez días desde la recepción de la notificación, el cesionario que mantuviera el tratamiento de los datos, deberá proceder a la rectificación y cancelación notificada.

Esta actualización de los datos de carácter personal no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Lo dispuesto en este apartado se entiende sin perjuicio de las facultades que a los afectados reconoce el título III de este reglamento.

6. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

No obstante, podrán conservarse durante el tiempo en que pueda exigirse algún tipo de responsabilidad derivada de una relación u obligación jurídica o de la ejecución de un contrato o de la aplicación de medidas precontractuales solicitadas por el interesado.

Una vez cumplido el período al que se refieren los párrafos anteriores, los datos sólo podrán ser conservados previa disociación de los mismos, sin perjuicio de la obligación de bloqueo prevista en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

7. Los datos de carácter personal serán tratados de forma que permitan el ejercicio del derecho de acceso, en tanto no proceda su cancelación.

Artículo 9. *Tratamiento con fines estadísticos, históricos o científicos.*

1. No se considerará incompatible, a los efectos previstos en el apartado 3 del artículo anterior, el tratamiento de los datos de carácter personal con fines históricos, estadísticos o científicos.

Para la determinación de los fines a los que se refiere el párrafo anterior se estará a la legislación que en cada caso resulte aplicable y, en particular, a lo dispuesto en la Ley 12/1989, de 9 de mayo, Reguladora de la función estadística pública, la Ley 16/1985, de 25 junio, del Patrimonio histórico español y la Ley 13/1986, de 14 de abril de Fomento y coordinación general de la investigación científica y técnica, y sus respectivas disposiciones de desarrollo, así como a la normativa autonómica en estas materias.

2. Por vía de excepción a lo dispuesto en el apartado 6 del artículo anterior, la Agencia Española de Protección de Datos o, en su caso, las autoridades de control de las comunidades autónomas podrán, previa solicitud del responsable del tratamiento y conforme al procedimiento establecido en la sección segunda del capítulo VII del título IX del presente reglamento, acordar el mantenimiento íntegro de determinados datos, atendidos sus valores históricos, estadísticos o científicos de acuerdo con las normas a las que se refiere el apartado anterior.

Artículo 10. *Supuestos que legitiman el tratamiento o cesión de los datos.*

1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello.

2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando:

a) Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes:

El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados previstos en el artículo 1 de la Ley Orgánica 15/1999, de 13 de diciembre.

El tratamiento o la cesión de los datos sean necesarios para que el responsable del tratamiento cumpla un deber que le imponga una de dichas normas.

b) **(Anulado)**

3. Los datos de carácter personal podrán tratarse sin necesidad del consentimiento del interesado cuando:

a) Se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de las competencias que les atribuya una norma con rango de ley o una norma de derecho comunitario.

b) Se recaben por el responsable del tratamiento con ocasión de la celebración de un contrato o precontrato o de la existencia de una relación negocial, laboral o administrativa de la que sea parte el afectado y sean necesarios para su mantenimiento o cumplimiento.

c) El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del apartado 6 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre.

4. Será posible la cesión de los datos de carácter personal sin contar con el consentimiento del interesado cuando:

a) La cesión responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control comporte la comunicación de los datos. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

b) La comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas o a las instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas y se realice en el ámbito de las funciones que la ley les atribuya expresamente.

c) La cesión entre Administraciones públicas cuando concurra uno de los siguientes supuestos:

Tenga por objeto el tratamiento de los datos con fines históricos, estadísticos o científicos.

Los datos de carácter personal hayan sido recogidos o elaborados por una Administración pública con destino a otra.

La comunicación se realice para el ejercicio de competencias idénticas o que versen sobre las mismas materias.

5. Los datos especialmente protegidos podrán tratarse y cederse en los términos previstos en los artículos 7 y 8 de la Ley Orgánica 15/1999, de 13 de diciembre.

En particular, no será necesario el consentimiento del interesado para la comunicación de datos personales sobre la salud, incluso a través de medios electrónicos, entre organismos, centros y servicios del Sistema Nacional de Salud cuando se realice para la atención sanitaria de las personas, conforme a lo dispuesto en el Capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud.

Artículo 11. *Verificación de datos en solicitudes formuladas a las Administraciones públicas.*

(Anulado)

CAPÍTULO II

Consentimiento para el tratamiento de los datos y deber de información

Sección 1.ª Obtención del consentimiento del afectado

Artículo 12. *Principios generales.*

1. El responsable del tratamiento deberá obtener el consentimiento del interesado para el tratamiento de sus datos de carácter personal salvo en aquellos supuestos en que el mismo no sea exigible con arreglo a lo dispuesto en las leyes.

La solicitud del consentimiento deberá ir referida a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba, así como de las restantes condiciones que concurran en el tratamiento o serie de tratamientos.

2. Cuando se solicite el consentimiento del afectado para la cesión de sus datos, éste deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos respecto de cuya comunicación se solicita el consentimiento y el tipo de actividad desarrollada por el cesionario. En caso contrario, el consentimiento será nulo.

3. Corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

Artículo 13. *Consentimiento para el tratamiento de datos de menores de edad.*

1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.

2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos.

No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior.

3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo.

4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

Artículo 14. *Forma de recabar el consentimiento.*

1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos.

2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal.

En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible.

3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud.

Artículo 15. *Solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma.*

Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

En particular, se entenderá cumplido tal deber cuando se permita al afectado la marcación de una casilla claramente visible y que no se encuentre ya marcada en el documento que se le entregue para la celebración del contrato o se establezca un procedimiento equivalente que le permita manifestar su negativa al tratamiento.

Artículo 16. *Tratamiento de datos de facturación y tráfico en servicios de comunicaciones electrónicas.*

La solicitud del consentimiento para el tratamiento o cesión de los datos de tráfico, facturación y localización por parte de los sujetos obligados, o en su caso la revocación de aquél, según la legislación reguladora de las telecomunicaciones se someterá a lo establecido en su normativa específica y, en lo que no resulte contrario a la misma, a lo establecido en la presente sección.

Artículo 17. *Revocación del consentimiento.*

1. El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado.

2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud.

4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre.

Sección 2.ª Deber de información al interesado

Artículo 18. *Acreditación del cumplimiento del deber de información.*

(Anulado)

Artículo 19. *Supuestos especiales.*

En los supuestos en que se produzca una modificación del responsable del fichero como consecuencia de una operación de fusión, escisión, cesión global de activos y pasivos, aportación o transmisión de negocio o rama de actividad empresarial, o cualquier operación de reestructuración societaria de análoga naturaleza, contemplada por la normativa mercantil, no se producirá cesión de datos, sin perjuicio del cumplimiento por el responsable de lo dispuesto en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Encargado del tratamiento

Artículo 20. *Relaciones entre el responsable y el encargado del tratamiento.*

1. El acceso a los datos por parte de un encargado del tratamiento que resulte necesario para la prestación de un servicio al responsable no se considerará comunicación de datos, siempre y cuando se cumpla lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente capítulo.

El servicio prestado por el encargado del tratamiento podrá tener o no carácter remunerado y ser temporal o indefinido.

No obstante, se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado.

2. Cuando el responsable del tratamiento contrate la prestación de un servicio que comporte un tratamiento de datos personales sometido a lo dispuesto en este capítulo deberá velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en este Reglamento.

3. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato al que se refiere el apartado 2 del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

No obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.

Artículo 21. *Posibilidad de subcontratación de los servicios.*

1. El encargado del tratamiento no podrá subcontratar con un tercero la realización de ningún tratamiento que le hubiera encomendado el responsable del tratamiento, salvo que hubiera obtenido de éste autorización para ello. En este caso, la contratación se efectuará siempre en nombre y por cuenta del responsable del tratamiento.

2. No obstante lo dispuesto en el apartado anterior, será posible la subcontratación sin necesidad de autorización siempre y cuando se cumplan los siguientes requisitos:

a) Que se especifiquen en el contrato los servicios que puedan ser objeto de subcontratación y, si ello fuera posible, la empresa con la que se vaya a subcontratar.

Cuando no se identificase en el contrato la empresa con la que se vaya a subcontratar, será preciso que el encargado del tratamiento comunique al responsable los datos que la identifiquen antes de proceder a la subcontratación.

b) Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones del responsable del fichero.

c) Que el encargado del tratamiento y la empresa subcontratista formalicen el contrato, en los términos previstos en el artículo anterior.

En este caso, el subcontratista será considerado encargado del tratamiento, siéndole de aplicación lo previsto en el artículo 20.3 de este reglamento.

3. Si durante la prestación del servicio resultase necesario subcontratar una parte del mismo y dicha circunstancia no hubiera sido prevista en el contrato, deberán someterse al responsable del tratamiento los extremos señalados en el apartado anterior.

Artículo 22. *Conservación de los datos por el encargado del tratamiento.*

1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

TÍTULO III

Derechos de acceso, rectificación, cancelación y oposición

CAPÍTULO I

Disposiciones generales

Artículo 23. *Carácter personalísimo.*

1. Los derechos de acceso, rectificación, cancelación y oposición son personalísimos y serán ejercidos por el afectado.

2. Tales derechos se ejercitarán:

a) Por el afectado, acreditando su identidad, del modo previsto en el artículo siguiente.

b) Cuando el afectado se encuentre en situación de incapacidad o minoría de edad que le imposibilite el ejercicio personal de estos derechos, podrán ejercitarse por su representante legal, en cuyo caso será necesario que acredite tal condición.

c) Los derechos también podrán ejercitarse a través de representante voluntario, expresamente designado para el ejercicio del derecho. En ese caso, deberá constar claramente acreditada la identidad del representado, mediante la aportación de copia de su Documento Nacional de Identidad o documento equivalente, y la representación conferida por aquél.

Cuando el responsable del fichero sea un órgano de las Administraciones públicas o de la Administración de Justicia, podrá acreditarse la representación por cualquier medio válido en derecho que deje constancia fidedigna, o mediante declaración en comparecencia personal del interesado.

3. Los derechos serán denegados cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma actúa en representación de aquél.

Artículo 24. *Condiciones generales para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. Los derechos de acceso, rectificación, cancelación y oposición son derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

2. Deberá concederse al interesado un medio sencillo y gratuito para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.

3. El ejercicio por el afectado de sus derechos de acceso, rectificación, cancelación y oposición será gratuito y en ningún caso podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar sus derechos el envío de cartas certificadas o semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

4. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a su público o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios. En tal caso, la identidad del interesado se considerará acreditada por los medios establecidos para la identificación de los clientes del responsable en la prestación de sus servicios o contratación de sus productos.

5. El responsable del fichero o tratamiento deberá atender la solicitud de acceso, rectificación, cancelación u oposición ejercida por el afectado aún cuando el mismo no hubiese utilizado el procedimiento establecido específicamente al efecto por aquél, siempre que el interesado haya utilizado un medio que permita acreditar el envío y la recepción de la solicitud, y que ésta contenga los elementos referidos en el párrafo 1 del artículo siguiente.

Artículo 25. *Procedimiento.*

1. Salvo en el supuesto referido en el párrafo 4 del artículo anterior, el ejercicio de los derechos deberá llevarse a cabo mediante comunicación dirigida al responsable del fichero, que contendrá:

a) Nombre y apellidos del interesado; fotocopia de su documento nacional de identidad, o de su pasaporte u otro documento válido que lo identifique y, en su caso, de la persona que lo represente, o instrumentos electrónicos equivalentes; así como el documento o instrumento electrónico acreditativo de tal representación. La utilización de firma electrónica identificativa del afectado eximirá de la presentación de las fotocopias del DNI o documento equivalente.

El párrafo anterior se entenderá sin perjuicio de la normativa específica aplicable a la comprobación de datos de identidad por las Administraciones Públicas en los procedimientos administrativos.

b) Petición en que se concreta la solicitud.

c) Dirección a efectos de notificaciones, fecha y firma del solicitante.

d) Documentos acreditativos de la petición que formula, en su caso.

2. El responsable del tratamiento deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros.

3. En el caso de que la solicitud no reúna los requisitos especificados en el apartado primero, el responsable del fichero deberá solicitar la subsanación de los mismos.

4. La respuesta deberá ser conforme con los requisitos previstos para cada caso en el presente título.

5. Corresponderá al responsable del tratamiento la prueba del cumplimiento del deber de respuesta al que se refiere el apartado 2, debiendo conservar la acreditación del cumplimiento del mencionado deber.

6. El responsable del fichero deberá adoptar las medidas oportunas para garantizar que las personas de su organización que tienen acceso a datos de carácter personal puedan informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

7. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición podrá modularse por razones de seguridad pública en los casos y con el alcance previsto en las Leyes.

8. Cuando las leyes aplicables a determinados ficheros concretos establezcan un procedimiento especial para la rectificación o cancelación de los datos contenidos en los mismos, se estará a lo dispuesto en aquéllas.

Artículo 26. *Ejercicio de los derechos ante un encargado del tratamiento.*

Cuando los afectados ejercitasen sus derechos ante un encargado del tratamiento y solicitasen el ejercicio de su derecho ante el mismo, el encargado deberá dar traslado de la solicitud al responsable, a fin de que por el mismo se resuelva, a menos que en la relación existente con el responsable del tratamiento se prevea precisamente que el encargado atenderá, por cuenta del responsable, las solicitudes de ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación u oposición.

CAPÍTULO II

Derecho de acceso

Artículo 27. *Derecho de acceso.*

1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento.

No obstante, cuando razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos.

3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

Artículo 28. *Ejercicio del derecho de acceso.*

1. Al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero:

a) Visualización en pantalla.
b) Escrito, copia o fotocopia remitida por correo, certificado o no.
c) Telecopia.
d) Correo electrónico u otros sistemas de comunicaciones electrónicas.
e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

2. Los sistemas de consulta del fichero previstos en el apartado anterior podrán restringirse en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que el que se ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.
3. El responsable del fichero deberá cumplir al facilitar el acceso lo establecido en el Título VIII de este Reglamento.

Si tal responsable ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el afectado lo rechazase, aquél no responderá por los posibles riesgos que para la seguridad de la información pudieran derivarse de la elección.
Del mismo modo, si el responsable ofreciera un procedimiento para hacer efectivo el derecho de acceso y el afectado exigiese que el mismo se materializase a través de un procedimiento que implique un coste desproporcionado, surtiendo el mismo efecto y garantizando la misma seguridad el procedimiento ofrecido por el responsable, serán de cuenta del afectado los gastos derivados de su elección.

Artículo 29. *Otorgamiento del acceso.*

1. El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición de acceso, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.
En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.
2. Si la solicitud fuera estimada y el responsable no acompañase a su comunicación la información a la que se refiere el artículo 27.1, el acceso se hará efectivo durante los diez días siguientes a dicha comunicación.
3. La información que se proporcione, cualquiera que sea el soporte en que fuere facilitada, se dará en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
Dicha información comprenderá todos los datos de base del afectado, los resultantes de cualquier elaboración o proceso informático, así como la información disponible sobre el origen de los datos, los cesionarios de los mismos y la especificación de los concretos usos y finalidades para los que se almacenaron los datos.

Artículo 30. *Denegación del acceso.*

1. El responsable del fichero o tratamiento podrá denegar el acceso a los datos de carácter personal cuando el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud, salvo que se acredite un interés legítimo al efecto.
2. Podrá también denegarse el acceso en los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Derechos de rectificación y cancelación

Artículo 31. *Derechos de rectificación y cancelación.*

1. El derecho de rectificación es el derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

2. El ejercicio del derecho de cancelación dará lugar a que se supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo conforme a este reglamento.

En los supuestos en que el interesado invoque el ejercicio del derecho de cancelación para revocar el consentimiento previamente prestado, se estará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre y en el presente reglamento.

Artículo 32. *Ejercicio de los derechos de rectificación y cancelación.*

1. La solicitud de rectificación deberá indicar a qué datos se refiere y la corrección que haya de realizarse y deberá ir acompañada de la documentación justificativa de lo solicitado.

En la solicitud de cancelación, el interesado deberá indicar a qué datos se refiere, aportando al efecto la documentación que lo justifique, en su caso.

2. El responsable del fichero resolverá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal del afectado deberá igualmente comunicárselo en el mismo plazo.

3. Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

La rectificación o cancelación efectuada por el cesionario no requerirá comunicación alguna al interesado, sin perjuicio del ejercicio de los derechos por parte de los interesados reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 33. *Denegación de los derechos de rectificación y cancelación.*

1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos.

2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.

3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO IV

Derecho de oposición

Artículo 34. *Derecho de oposición.*

El derecho de oposición es el derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los siguientes supuestos:

a) Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique, siempre que una Ley no disponga lo contrario.

b) Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial, en los términos previstos en el artículo 51 de este reglamento, cualquiera que sea la empresa responsable de su creación.

c) Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal, en los términos previstos en el artículo 36 de este reglamento.

Artículo 35. *Ejercicio del derecho de oposición.*

1. El derecho de oposición se ejercitará mediante solicitud dirigida al responsable del tratamiento.

Cuando la oposición se realice con base en la letra a) del artículo anterior, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. El responsable del fichero resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

En el caso de que no disponga de datos de carácter personal de los afectados deberá igualmente comunicárselo en el mismo plazo.

3. El responsable del fichero o tratamiento deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto en el apartado 2 de este artículo.

Artículo 36. *Derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos.*

1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta.

2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión:

a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato.

b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado.

TÍTULO IV

Disposiciones aplicables a determinados ficheros de titularidad privada

CAPÍTULO I

Ficheros de información sobre solvencia patrimonial y crédito

Sección 1.ª Disposiciones generales

Artículo 37. *Régimen aplicable.*

1. El tratamiento de datos de carácter personal sobre solvencia patrimonial y crédito, previsto en el apartado 1 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, se

someterá a lo establecido, con carácter general, en dicha ley orgánica y en el presente reglamento.

2. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición en el caso de los ficheros a que se refiere el apartado anterior, se rige por lo dispuesto en los capítulos I a IV del título III del presente reglamento, con los siguientes criterios:

a) Cuando la petición de ejercicio de los derechos se dirigiera al responsable del fichero, éste estará obligado a satisfacer, en cualquier caso, dichos derechos.

b) Si la petición se dirigiera a las personas y entidades a las que se presta el servicio, éstas únicamente deberán comunicar al afectado aquellos datos relativos al mismo que les hayan sido comunicados y a facilitar la identidad del responsable para que, en su caso, puedan ejercitar sus derechos ante el mismo.

3. De conformidad con el apartado 2 del artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre, también podrán tratarse los datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés.

Estos datos deberán conservarse en ficheros creados con la exclusiva finalidad de facilitar información crediticia del afectado y su tratamiento se regirá por lo dispuesto en el presente reglamento y, en particular, por las previsiones contenidas en la sección segunda de este capítulo.

Sección 2.ª Tratamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés

Artículo 38. *Requisitos para la inclusión de los datos.*

1. Sólo será posible la inclusión en estos ficheros de datos de carácter personal que sean determinantes para enjuiciar la solvencia económica del afectado, siempre que concurran los siguientes requisitos:

a) Existencia previa de una deuda cierta, vencida, exigible, que haya resultado impagada **y respecto de la cual no se haya entablado reclamación judicial, arbitral o administrativa, o tratándose de servicios financieros, no se haya planteado una reclamación en los términos previstos en el Reglamento de los Comisionados para la defensa del cliente de servicios financieros, aprobado por Real Decreto 303/2004, de 20 de febrero.**

> Téngase en cuenta que se anula el inciso destacado de la letra a) del apartado 1 por Sentencias del TS de 15 de julio de 2010. Ref. BOE-A-2010-16299 y Ref. BOE-A-2010-16301

b) Que no hayan transcurrido seis años desde la fecha en que hubo de procederse al pago de la deuda o del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

c) Requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.

2. **(Anulado)**

3. El acreedor o quien actúe por su cuenta o interés estará obligado a conservar a disposición del responsable del fichero común y de la Agencia Española de Protección de Datos documentación suficiente que acredite el cumplimiento de los requisitos establecidos en este artículo y del requerimiento previo al que se refiere el artículo siguiente.

Artículo 39. *Información previa a la inclusión.*

El acreedor deberá informar al deudor, en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento al que se refiere la letra c) del apartado 1 del artículo anterior, que en caso de no producirse el pago en el término previsto para ello y cumplirse los requisitos previstos en el citado artículo, los datos relativos al impago podrán

ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

Artículo 40. *Notificación de inclusión.*

1. El responsable del fichero común deberá notificar a los interesados respecto de los que hayan registrado datos de carácter personal, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos, informándole asimismo de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, en los términos establecidos por la Ley Orgánica 15/1999, de 13 de diciembre.

2. Se efectuará una notificación por cada deuda concreta y determinada con independencia de que ésta se tenga con el mismo o con distintos acreedores.

3. La notificación deberá efectuarse a través de un medio fiable, auditable e independiente de la entidad notificante, que la permita acreditar la efectiva realización de los envíos.

4. En todo caso, será necesario que el responsable del fichero pueda conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado.

No se entenderán suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

5. Si la notificación de inclusión fuera devuelta, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

Artículo 41. *Conservación de los datos.*

1. Sólo podrán ser objeto de tratamiento los datos que respondan con veracidad a la situación de la deuda en cada momento concreto.

El pago o cumplimiento de la deuda determinará la cancelación inmediata de todo dato relativo a la misma.

2. En los restantes supuestos, los datos deberán ser cancelados cuando se hubieran cumplido seis años contados a partir del vencimiento de la obligación o del plazo concreto si aquélla fuera de vencimiento periódico.

Artículo 42. *Acceso a la información contenida en el fichero.*

1. Los datos contenidos en el fichero común sólo podrán ser consultados por terceros cuando precisen enjuiciar la solvencia económica del afectado. En particular, se considerará que concurre dicha circunstancia en los siguientes supuestos:

a) Que el afectado mantenga con el tercero algún tipo de relación contractual que aún no se encuentre vencida.

b) Que el afectado pretenda celebrar con el tercero un contrato que implique el pago aplazado del precio.

c) Que el afectado pretenda contratar con el tercero la prestación de un servicio de facturación periódica.

2. Los terceros deberán informar por escrito a las personas en las que concurran los supuestos contemplados en las letras b) y c) precedentes de su derecho a consultar el fichero.

En los supuestos de contratación telefónica de los productos o servicios a los que se refiere el párrafo anterior, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

Artículo 43. *Responsabilidad.*

1. El acreedor o quien actúe por su cuenta o interés deberá asegurarse que concurren todos los requisitos exigidos en los artículos 38 y 39 en el momento de notificar los datos adversos al responsable del fichero común.

2. El acreedor o quien actúe por su cuenta o interés será responsable de la inexistencia o inexactitud de los datos que hubiera facilitado para su inclusión en el fichero, en los términos previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 44. *Ejercicio de los derechos de acceso, rectificación, cancelación y oposición.*

1. El ejercicio de los derechos de acceso, rectificación, cancelación y oposición se rige por lo dispuesto en los capítulos I a IV del título III de este reglamento, sin perjuicio de lo señalado en el presente artículo.

2. Cuando el interesado ejercite su derecho de acceso en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirigiera al titular del fichero común, éste deberá comunicar al afectado todos los datos relativos al mismo que obren en el fichero.

En este caso, el titular del fichero común deberá, además de dar cumplimiento a lo establecido en el presente reglamento, facilitar las evaluaciones y apreciaciones que sobre el afectado se hayan comunicado en los últimos seis meses y el nombre y dirección de los cesionarios.

2.ª Si la solicitud se dirigiera a cualquier otra entidad participante en el sistema, deberá comunicar al afectado todos los datos relativos al mismo a los que ella pueda acceder, así como la identidad y dirección del titular del fichero común para que pueda completar el ejercicio de su derecho de acceso.

3. Cuando el interesado ejercite sus derechos de rectificación o cancelación en relación con la inclusión de sus datos en un fichero regulado por el artículo 29.2 de la Ley Orgánica 15/1999, de 13 de diciembre, se tendrán en cuenta las siguientes reglas:

1.ª Si la solicitud se dirige al titular del fichero común, éste tomará las medidas oportunas para trasladar dicha solicitud a la entidad que haya facilitado los datos, para que ésta la resuelva. En el caso de que el responsable del fichero común no haya recibido contestación por parte de la entidad en el plazo de siete días, procederá a la rectificación o cancelación cautelar de los mismos.

2.ª Si la solicitud se dirige a quien haya facilitado los datos al fichero común procederá a la rectificación o cancelación de los mismos en sus ficheros y a notificarlo al titular del fichero común en el plazo de diez días, dando asimismo respuesta al interesado en los términos previstos en el artículo 33 de este reglamento.

3.ª Si la solicitud se dirige a otra entidad participante en el sistema, que no hubiera facilitado al fichero común los datos, dicha entidad informará al afectado sobre este hecho en el plazo máximo de diez días, proporcionándole, además, la identidad y dirección del titular del fichero común para, que en su caso, puedan ejercitar sus derechos ante el mismo.

CAPÍTULO II

Tratamientos para actividades de publicidad y prospección comercial

Artículo 45. *Datos susceptibles de tratamiento e información al interesado.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, así como quienes realicen estas actividades con el fin de comercializar sus propios productos o servicios o los de terceros, sólo podrán utilizar nombres y direcciones u otros datos de carácter personal cuando los mismos se encuentren en uno de los siguientes casos:

a) Figuren en alguna de las fuentes accesibles al público a las que se refiere la letra j) del artículo 3 de la Ley Orgánica 15/1999, de 13 de diciembre y el artículo 7 de este

reglamento y el interesado no haya manifestado su negativa u oposición a que sus datos sean objeto de tratamiento para las actividades descritas en este apartado.

b) Hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

2. Cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, deberá informarse al interesado en cada comunicación que se le dirija del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten, con indicación de ante quién podrán ejercitarse.

A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos.

Artículo 46. *Tratamiento de datos en campañas publicitarias.*

1. Para que una entidad pueda realizar por sí misma una actividad publicitaria de sus productos o servicios entre sus clientes será preciso que el tratamiento se ampare en alguno de los supuestos contemplados en el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre.

2. En caso de que una entidad contrate o encomiende a terceros la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

a) Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrate la campaña, ésta será responsable del tratamiento de los datos.

b) Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsable del tratamiento.

c) Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

3. En el supuesto contemplado en el apartado anterior, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

4. A los efectos previstos en este artículo, se consideran parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Artículo 47. *Depuración de datos personales.*

Cuando dos o más responsables por sí mismos o mediante encargo a terceros pretendieran constatar sin consentimiento de los afectados, con fines de promoción o comercialización de sus productos o servicios y mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos, el tratamiento así realizado constituirá una cesión o comunicación de datos.

Artículo 48. *Ficheros de exclusión del envío de comunicaciones comerciales.*

Los responsables a los que el afectado haya manifestado su negativa a recibir publicidad podrán conservar los mínimos datos imprescindibles para identificarlo y adoptar las medidas necesarias que eviten el envío de publicidad.

Artículo 49. *Ficheros comunes de exclusión del envío de comunicaciones comerciales.*

1. Será posible la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para

evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

A tal efecto, los citados ficheros podrán contener los mínimos datos imprescindibles para identificar al afectado.

2. Cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

3. La entidad responsable del fichero común podrá tratar los datos de los interesados que hubieran manifestado su negativa u oposición al tratamiento de sus datos con fines de publicidad o prospección comercial, cumpliendo las restantes obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento.

4. Quienes pretendan efectuar un tratamiento relacionado con actividades de publicidad o prospección comercial deberán previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

Artículo 50. *Derechos de acceso, rectificación y cancelación.*

1. El ejercicio de los derechos de acceso, rectificación y cancelación en relación con los tratamientos vinculados a actividades de publicidad y prospección comercial se someterá a lo previsto en los capítulos I a IV del título III de este reglamento.

2. Si el derecho se ejercitase ante una entidad que hubiese encargado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo otorgue al afectado su derecho en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 51. *Derecho de oposición.*

1. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

La oposición a la que se refiere el párrafo anterior deberá entenderse sin perjuicio del derecho del interesado a revocar cuando lo estimase oportuno el consentimiento que hubiera otorgado, en su caso, para el tratamiento de los datos.

2. A tal efecto, deberá concederse al interesado un medio sencillo y gratuito para oponerse al tratamiento. En particular, se considerará cumplido lo dispuesto en este precepto cuando los derechos puedan ejercitarse mediante la llamada a un número telefónico gratuito o la remisión de un correo electrónico.

3. Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la atención a sus clientes o el ejercicio de reclamaciones relacionadas con el servicio prestado o los productos ofertados al mismo, deberá concederse la posibilidad al afectado de ejercer su oposición a través de dichos servicios.

No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable del tratamiento establezca como medio para que el interesado pueda ejercitar su oposición el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste excesivo para el interesado.

En todo caso, el ejercicio por el afectado de sus derechos no podrá suponer un ingreso adicional para el responsable del tratamiento ante el que se ejercitan.

4. Si el derecho de oposición se ejercitase ante una entidad que hubiera encomendado a un tercero la realización de una campaña publicitaria, aquélla estará obligada, en el plazo de diez días, desde la recepción de la comunicación de la solicitud de ejercicio de derechos del afectado, a comunicar la solicitud al responsable del fichero a fin de que el mismo atienda el derecho del afectado en el plazo de diez días desde la recepción de la comunicación, dando cuenta de ello al afectado.

Lo dispuesto en el párrafo anterior se entenderá sin perjuicio del deber impuesto a la entidad mencionada en el apartado anterior, en todo caso, por el párrafo segundo del artículo 5.5 de la Ley Orgánica 15/1999, de 13 de diciembre.

TÍTULO V

Obligaciones previas al tratamiento de los datos

CAPÍTULO I

Creación, modificación o supresión de ficheros de titularidad pública

Artículo 52. *Disposición o Acuerdo de creación, modificación o supresión del fichero.*

1. La creación, modificación o supresión de los ficheros de titularidad pública sólo podrá hacerse por medio de disposición general o acuerdo publicados en el «Boletín Oficial del Estado» o diario oficial correspondiente.

2. En todo caso, la disposición o acuerdo deberá dictarse y publicarse con carácter previo a la creación, modificación o supresión del fichero.

Artículo 53. *Forma de la disposición o acuerdo.*

1. Cuando la disposición se refiera a los órganos de la Administración General del Estado o a las entidades u organismos vinculados o dependientes de la misma, deberá revestir la forma de orden ministerial o resolución del titular de la entidad u organismo correspondiente.

2. En el caso de los órganos constitucionales del Estado, se estará a lo que establezcan sus normas reguladoras.

3. En relación con los ficheros de los que sean responsables las comunidades autónomas, entidades locales y las entidades u organismos vinculados o dependientes de las mismas, las universidades públicas, así como los órganos de las comunidades autónomas con funciones análogas a los órganos constitucionales del Estado, se estará a su legislación específica.

4. La creación, modificación o supresión de los ficheros de los que sean responsables las corporaciones de derecho público y que se encuentren relacionados con el ejercicio por aquéllas de potestades de derecho público deberá efectuarse a través de acuerdo de sus órganos de gobierno, en los términos que establezcan sus respectivos Estatutos, debiendo ser igualmente objeto de publicación en el «Boletín Oficial del Estado» o diario oficial correspondiente.

Artículo 54. *Contenido de la disposición o acuerdo.*

1. La disposición o acuerdo de creación del fichero deberá contener los siguientes extremos:

a) La identificación del fichero o tratamiento, indicando su denominación, así como la descripción de su finalidad y usos previstos.

b) El origen de los datos, indicando el colectivo de personas sobre los que se pretende obtener datos de carácter personal o que resulten obligados a suministrarlos, el procedimiento de recogida de los datos y su procedencia.

c) La estructura básica del fichero mediante la descripción detallada de los datos identificativos, y en su caso, de los datos especialmente protegidos, así como de las

restantes categorías de datos de carácter personal incluidas en el mismo y el sistema de tratamiento utilizado en su organización.

d) Las comunicaciones de datos previstas, indicando en su caso, los destinatarios o categorías de destinatarios.

e) Las transferencias internacionales de datos previstas a terceros países, con indicación, en su caso, de los países de destino de los datos.

f) Los órganos responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) El nivel básico, medio o alto de seguridad que resulte exigible, de acuerdo con lo establecido en el título VIII del presente reglamento.

2. La disposición o acuerdo de modificación del fichero deberá indicar las modificaciones producidas en cualquiera de los extremos a los que se refiere el apartado anterior.

3. En las disposiciones o acuerdos que se dicten para la supresión de los ficheros se establecerá el destino que vaya a darse a los datos o, en su caso, las previsiones que se adopten para su destrucción.

CAPÍTULO II

Notificación e inscripción de los ficheros de titularidad pública o privada

Artículo 55. *Notificación de ficheros.*

1. Todo fichero de datos de carácter personal de titularidad pública será notificado a la Agencia Española de Protección de Datos por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el diario oficial correspondiente.

2. Los ficheros de datos de carácter personal de titularidad privada serán notificados a la Agencia Española de Protección de Datos por la persona o entidad privada que pretenda crearlos, con carácter previo a su creación. La notificación deberá indicar la identificación del responsable del fichero, la identificación del fichero, sus finalidades y los usos previstos, el sistema de tratamiento empleado en su organización, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, la indicación del nivel de medidas de seguridad básico, medio o alto exigible, y en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales de datos.

3. Cuando la obligación de notificar afecte a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, la notificación se realizará a la autoridad autonómica competente, que dará traslado de la inscripción al Registro General de Protección de Datos.

El Registro General de Protección de Datos podrá solicitar de las autoridades de control de las comunidades autónomas el traslado al que se refiere el párrafo anterior, procediendo, en su defecto, a la inclusión de oficio del fichero en el Registro.

4. La notificación se realizará conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

Artículo 56. *Tratamiento de datos en distintos soportes.*

1. La notificación de un fichero de datos de carácter personal es independiente del sistema de tratamiento empleado en su organización y del soporte o soportes empleados para el tratamiento de los datos.

2. Cuando los datos de carácter personal objeto de un tratamiento estén almacenados en diferentes soportes, automatizados y no automatizados o exista una copia en soporte no automatizado de un fichero automatizado sólo será precisa una sola notificación, referida a dicho fichero.

Artículo 57. *Ficheros en los que exista más de un responsable.*

Cuando se tenga previsto crear un fichero del que resulten responsables varias personas o entidades simultáneamente, cada una de ellas deberá notificar, a fin de proceder a su inscripción en el Registro General de Protección de Datos y, en su caso, en los Registros de Ficheros creados por las autoridades de control de las comunidades autónomas, la creación del correspondiente fichero.

Artículo 58. *Notificación de la modificación o supresión de ficheros.*

1. La inscripción del fichero deberá encontrarse actualizada en todo momento. Cualquier modificación que afecte al contenido de la inscripción de un fichero deberá ser previamente notificada a la Agencia Española de Protección de Datos o a las autoridades de control autonómicas competentes, a fin de proceder a su inscripción en el registro correspondiente, conforme a lo dispuesto en el artículo 55.

2. Cuando el responsable del fichero decida su supresión, deberá notificarla a efectos de que se proceda a la cancelación de la inscripción en el registro correspondiente.

3. Tratándose de ficheros de titularidad pública, cuando se pretenda la modificación que afecte a alguno de los requisitos previstos en el artículo 55 o la supresión del fichero deberá haberse adoptado, con carácter previo a la notificación la correspondiente norma o acuerdo en los términos previstos en el capítulo I de este título.

Artículo 59. *Modelos y soportes para la notificación.*

1. La Agencia Española de Protección de Datos publicará mediante la correspondiente Resolución del Director los modelos o formularios electrónicos de notificación de creación, modificación o supresión de ficheros, que permitan su presentación a través de medios telemáticos o en soporte papel, así como, previa consulta de las autoridades de protección de datos de las comunidades autónomas, los formatos para la comunicación telemática de ficheros públicos por las autoridades de control autonómicas, de conformidad con lo establecido en los artículos 55 y 58 del presente reglamento.

2. Los modelos o formularios electrónicos de notificación se podrán obtener gratuitamente en la página web de la Agencia Española de Protección de Datos.

3. El Director de la Agencia Española de Protección de Datos podrá establecer procedimientos simplificados de notificación en atención a las circunstancias que concurran en el tratamiento o el tipo de fichero al que se refiera la notificación.

Artículo 60. *Inscripción de los ficheros.*

1. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución acordando, en su caso, la inscripción, una vez tramitado el procedimiento previsto en el capítulo IV del título IX.

2. La inscripción contendrá el código asignado por el Registro, la identificación del responsable del fichero, la identificación del fichero o tratamiento, la descripción de su finalidad y usos previstos, el sistema de tratamiento empleado en su organización, en su caso, el colectivo de personas sobre el que se obtienen los datos, el procedimiento y procedencia de los datos, las categorías de datos, el servicio o unidad de acceso, y la indicación del nivel de medidas de seguridad exigible conforme a lo dispuesto en el artículo 81.

Asimismo, se incluirán, en su caso, la identificación del encargado del tratamiento en donde se encuentre ubicado el fichero y los destinatarios de cesiones y transferencias internacionales.

En el caso de ficheros de titularidad pública también se hará constar la referencia de la disposición general por la que ha sido creado, y en su caso, modificado.

3. La inscripción de un fichero en el Registro General de Protección de Datos, no exime al responsable del cumplimiento del resto de las obligaciones previstas en la Ley Orgánica 15/1999, de 13 de diciembre, y demás disposiciones reglamentarias.

Artículo 61. *Cancelación de la inscripción.*

1. Cuando el responsable del tratamiento comunicase, en virtud de lo dispuesto en el artículo 58 de este reglamento, la supresión del fichero, el Director de la Agencia Española de Protección de Datos, previa la tramitación del procedimiento establecido en la sección primera del capítulo IV del título IX, dictará resolución acordando la cancelación de la inscripción correspondiente al fichero.

2. El Director de la Agencia Española de Protección de Datos podrá, en ejercicio de sus competencias, acordar de oficio la cancelación de la inscripción de un fichero cuando concurran circunstancias que acrediten la imposibilidad de su existencia, previa la tramitación del procedimiento establecido en la sección segunda del capítulo IV del título IX de este reglamento.

Artículo 62. *Rectificación de errores.*

El Registro General de Protección de Datos podrá rectificar en cualquier momento, de oficio o a instancia de los interesados, los errores materiales, de hecho o aritméticos que pudieran existir en las inscripciones, de conformidad con lo dispuesto en el artículo 105 de la Ley 30/1992, de 26 de noviembre.

Artículo 63. *Inscripción de oficio de ficheros de titularidad pública.*

1. En supuestos excepcionales con el fin de garantizar el derecho a la protección de datos de los afectados, y sin perjuicio de la obligación de notificación, se podrá proceder a la inscripción de oficio de un determinado fichero en el Registro General de Protección de Datos.

2. Para que lo dispuesto en el apartado anterior resulte de aplicación, será requisito indispensable que la correspondiente norma o acuerdo regulador de los ficheros que contengan datos de carácter personal haya sido publicado en el correspondiente diario oficial y cumpla los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

3. El Director de la Agencia Española de Protección de Datos podrá, a propuesta del Registro General de Protección de Datos, acordar la inscripción del fichero de titularidad pública en el Registro, notificándose dicho acuerdo al órgano responsable del fichero.

Cuando la inscripción se refiera a ficheros sujetos a la competencia de la autoridad de control de una comunidad autónoma que haya creado su propio registro de ficheros, se comunicará a la referida autoridad de control autonómica para que proceda, en su caso, a la inscripción de oficio.

Artículo 64. *Colaboración con las autoridades de control de las comunidades autónomas.*

El Director de la Agencia Española de Protección de Datos podrá celebrar con los directores de las autoridades de control de las comunidades autónomas los convenios de colaboración o acuerdos que estime pertinentes, a fin de garantizar la inscripción en el Registro General de Protección de Datos de los ficheros sometidos a la competencia de dichas autoridades autonómicas.

TÍTULO VI

Transferencias internacionales de datos

CAPÍTULO I

Disposiciones generales

Artículo 65. *Cumplimiento de las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre.*

La transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente reglamento.

Artículo 66. *Autorización y notificación.*

1. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento será necesaria la autorización del Director de la Agencia Española de Protección de Datos, que se otorgará en caso de que el exportador aporte las garantías a las que se refiere el artículo 70 del presente reglamento.

La autorización se otorgará conforme al procedimiento establecido en la sección primera del capítulo V del título IX de este reglamento.

2. La autorización no será necesaria:

a) Cuando el Estado en el que se encontrase el importador ofrezca un nivel adecuado de protección conforme a lo previsto en el capítulo II de este título.

b) Cuando la transferencia se encuentre en uno de los supuestos contemplados en los apartados a) a j) del artículo 34 de la Ley Orgánica 15/1999, de 13 de diciembre.

3. En todo caso, la transferencia internacional de datos deberá ser notificada a fin de proceder a su inscripción en el Registro General de Protección de Datos, conforme al procedimiento establecido en la sección primera del capítulo IV del título IX del presente reglamento.

CAPÍTULO II

Transferencias a estados que proporcionen un nivel adecuado de protección

Artículo 67. *Nivel adecuado de protección acordado por la Agencia Española de Protección de Datos.*

1. No será precisa autorización del Director de la Agencia Española de Protección de Datos a una transferencia internacional de datos cuando las normas aplicables al Estado en que se encontrase el importador ofrezcan dicho nivel adecuado de protección a juicio del Director de la Agencia Española de Protección de Datos.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se acordase que un determinado país proporciona un nivel adecuado de protección de datos serán publicadas en el «Boletín Oficial del Estado».

2. El Director de la Agencia Española de Protección de Datos acordará la publicación de la relación de países cuyo nivel de protección haya sido considerado equiparable conforme a lo dispuesto en el apartado anterior.

Esta lista se publicará y mantendrá actualizada asimismo a través de medios informáticos o telemáticos.

Artículo 68. *Nivel adecuado de protección declarado por Decisión de la Comisión Europea.*

No será necesaria la autorización del Director de la Agencia Española de Protección de Datos para la realización de una transferencia internacional de datos que tuvieran por importador una persona o entidad, pública o privada, situada en el territorio de un Estado respecto del que se haya declarado por la Comisión Europea la existencia de un nivel adecuado de protección.

Artículo 69. *Suspensión temporal de las transferencias.*

1. En los supuestos previstos en los artículos precedentes, el Director de la Agencia Española de Protección de Datos, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, podrá acordar, previa audiencia del exportador, la suspensión temporal de la transferencia de datos hacia un importador ubicado en un tercer Estado del que se haya declarado la existencia de un nivel adecuado de protección, cuando concurra alguna de las circunstancias siguientes:

a) Que las autoridades de Protección de Datos del Estado importador o cualquier otra competente, en caso de no existir las primeras, resuelvan que el importador ha vulnerado las normas de protección de datos establecidas en su derecho interno.

b) Que existan indicios racionales de que se estén vulnerando las normas o, en su caso, los principios de protección de datos por la entidad importadora de la transferencia y que las autoridades competentes en el Estado en que se encuentre el importador no han adoptado o no van a adoptar en el futuro las medidas oportunas para resolver el caso en cuestión, habiendo sido advertidas de la situación por la Agencia Española de Protección de Datos. En este caso se podrá suspender la transferencia cuando su continuación pudiera generar un riesgo inminente de grave perjuicio a los afectados.

2. La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

En estos casos, la decisión del Director de la Agencia Española de Protección de Datos será notificada a la Comisión Europea.

CAPÍTULO III

Transferencias a Estados que no proporcionen un nivel adecuado de protección

Artículo 70. *Transferencias sujetas a autorización del Director de la Agencia Española de Protección de Datos.*

1. Cuando la transferencia tenga por destino un Estado respecto del que no se haya declarado por la Comisión Europea o no se haya considerado por el Director de la Agencia Española de Protección de Datos que existe un nivel adecuado de protección, será necesario recabar la autorización del Director de la Agencia Española de Protección de Datos.

La autorización de la transferencia se tramitará conforme al procedimiento establecido en la sección primera del capítulo V del título IX del presente reglamento.

2. La autorización podrá ser otorgada en caso de que el responsable del fichero o tratamiento aporte un contrato escrito, celebrado entre el exportador y el importador, en el que consten las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos.

A tal efecto, se considerará que establecen las adecuadas garantías los contratos que se celebren de acuerdo con lo previsto en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de Junio de 2001, 2002/16/CE, de 27 de diciembre de 2001, y 2004/915/CE, de 27 de

diciembre de 2004 o de lo que dispongan las Decisiones de la Comisión que den cumplimiento a lo establecido en el artículo 26.4 de la Directiva 95/46/CE.

3. En el supuesto contemplado en el apartado anterior, el Director de la Agencia Española de Protección de Datos podrá denegar o, en uso de la potestad que le otorga el artículo 37.1 f) de la Ley Orgánica 15/1999, de 13 de diciembre, suspender temporalmente, previa audiencia del exportador, la transferencia, cuando concurra alguna de las circunstancias siguientes:

a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza.

b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo.

c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador.

d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos.

e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados.

La suspensión se acordará previa la tramitación del procedimiento establecido en la sección segunda del capítulo V del título IX del presente reglamento.

Las resoluciones del Director de la Agencia Española de Protección de Datos por las que se deniegue o suspenda una transferencia internacional de datos en virtud de las causas a las que se refiere este apartado serán notificadas a la Comisión de las Comunidades Europeas cuando así sea exigible.

4. También podrá otorgarse la autorización para la transferencia internacional de datos en el seno de grupos multinacionales de empresas cuando hubiesen sido adoptados por los mismos normas o reglas internas en que consten las necesarias garantías de respeto a la protección de la vida privada y el derecho fundamental a la protección de datos de los afectados y se garantice asimismo el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

En este caso, para que proceda la autorización del Director de la Agencia Española de Protección de Datos será preciso que las normas o reglas resulten vinculantes para las empresas del Grupo y exigibles conforme al ordenamiento jurídico español.

En todo caso, la autorización del Director de la Agencia Española de Protección de Datos implicará la exigibilidad de lo previsto en las normas o reglas internas tanto por la Agencia como por los afectados cuyos datos hubieran sido objeto de tratamiento.

TÍTULO VII

Códigos tipo

Artículo 71. *Objeto y naturaleza.*

1. Los códigos tipo a los que se refiere el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, tienen por objeto adecuar lo establecido en la citada Ley Orgánica y en el presente reglamento a las peculiaridades de los tratamientos efectuados por quienes se adhieren a los mismos.

A tal efecto, contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos, facilitar el ejercicio de los derechos de los afectados y favorecer el cumplimiento de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento.

2. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional y serán vinculantes para quienes se adhieran a los mismos.

Artículo 72. *Iniciativa y ámbito de aplicación.*

1. Los códigos tipo tendrán carácter voluntario.

2. Los códigos tipo de carácter sectorial podrán referirse a la totalidad o a parte de los tratamientos llevados a cabo por entidades pertenecientes a un mismo sector, debiendo ser formulados por organizaciones representativas de dicho sector, al menos en su ámbito territorial de aplicación, y sin perjuicio de la potestad de dichas entidades de ajustar el código tipo a sus peculiaridades.

3. Los códigos tipo promovidos por una empresa deberán referirse a la totalidad de los tratamientos llevados a cabo por la misma.

4. Las Administraciones públicas y las corporaciones de Derecho Público podrán adoptar códigos tipo de acuerdo con lo establecido en las normas que les sean aplicables.

Artículo 73. *Contenido.*

1. Los códigos tipo deberán estar redactados en términos claros y accesibles.

2. Los códigos tipo deben respetar la normativa vigente e incluir, como mínimo, con suficiente grado de precisión:

a) La delimitación clara y precisa de su ámbito de aplicación, las actividades a que el código se refiere y los tratamientos sometidos al mismo.

b) Las previsiones específicas para la aplicación de los principios de protección de datos.

c) El establecimiento de estándares homogéneos para el cumplimiento por los adheridos al código de las obligaciones establecidas en la Ley Orgánica 15/1999, de 13 de diciembre.

d) El establecimiento de procedimientos que faciliten el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

e) La determinación de las cesiones y transferencias internacionales de datos que, en su caso, se prevean, con indicación de las garantías que deban adoptarse.

f) Las acciones formativas en materia de protección de datos dirigidas a quienes los traten, especialmente en cuanto a su relación con los afectados.

g) Los mecanismos de supervisión a través de los cuales se garantice el cumplimiento por los adheridos de lo establecido en el código tipo, en los términos previstos en el artículo 74 de este reglamento.

3. En particular, deberán contenerse en el código:

a) Cláusulas tipo para la obtención del consentimiento de los afectados al tratamiento o cesión de sus datos.

b) Cláusulas tipo para informar a los afectados del tratamiento, cuando los datos no sean obtenidos de los mismos.

c) Modelos para el ejercicio por los afectados de sus derechos de acceso, rectificación, cancelación y oposición.

d) Modelos de cláusulas para el cumplimiento de los requisitos formales exigibles para la contratación de un encargado del tratamiento, en su caso.

Artículo 74. *Compromisos adicionales.*

1. Los códigos tipo podrán incluir cualquier otro compromiso adicional que asuman los adheridos para un mejor cumplimiento de la legislación vigente en materia de protección de datos.

2. Además podrán contener cualquier otro compromiso que puedan establecer las entidades promotoras y, en particular, sobre:

a) La adopción de medidas de seguridad adicionales a las exigidas por la Ley Orgánica 15/1999, de 13 de diciembre, y el presente Reglamento.

b) La identificación de las categorías de cesionarios o importadores de los datos.

c) Las medidas concretas adoptadas en materia de protección de los menores o de determinados colectivos de afectados.

d) El establecimiento de un sello de calidad que identifique a los adheridos al código.

Artículo 75. *Garantías del cumplimiento de los códigos tipo.*

1. Los códigos tipo deberán incluir procedimientos de supervisión independientes para garantizar el cumplimiento de las obligaciones asumidas por los adheridos, y establecer un régimen sancionador adecuado, eficaz y disuasorio.

2. El procedimiento que se prevea deberá garantizar:

a) La independencia e imparcialidad del órgano responsable de la supervisión.

b) La sencillez, accesibilidad, celeridad y gratuidad para la presentación de quejas y reclamaciones ante dicho órgano por los eventuales incumplimientos del código tipo.

c) El principio de contradicción.

d) Una graduación de sanciones que permita ajustarlas a la gravedad del incumplimiento. Esas sanciones deberán ser disuasorias y podrán implicar la suspensión de la adhesión al código o la expulsión de la entidad adherida. Asimismo, podrá establecerse, en su caso, su publicidad.

e) La notificación al afectado de la decisión adoptada.

3. Asimismo, y sin perjuicio de lo dispuesto en el artículo 19 de la Ley Orgánica 15/1999, de 13 de diciembre, los códigos tipo podrán contemplar procedimientos para la determinación de medidas reparadoras en caso de haberse causado un perjuicio a los afectados como consecuencia del incumplimiento del código tipo.

4. Lo dispuesto en este artículo se aplicará sin perjuicio de las competencias de la Agencia Española de Protección de Datos y, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 76. *Relación de adheridos.*

El código tipo deberá incorporar como anexo una relación de adheridos, que deberá mantenerse actualizada, a disposición de la Agencia Española de Protección de Datos.

Artículo 77. *Depósito y publicidad de los códigos tipo.*

1. Para que los códigos tipo puedan ser considerados como tales a los efectos previstos en el artículo 32 de la Ley Orgánica 15/1999, de 13 de diciembre, y el presente reglamento, deberán ser depositados e inscritos en el Registro General de Protección de Datos de la Agencia Española de Protección de Datos o, cuando corresponda, en el registro que fuera creado por las comunidades autónomas, que darán traslado para su inclusión al Registro General de Protección de Datos.

2. A tal efecto, los códigos tipo deberán ser presentados ante la correspondiente autoridad de control, tramitándose su inscripción, en caso de estar sometidos a la decisión de la Agencia Española de Protección de Datos, conforme al procedimiento establecido en el capítulo VI del título IX de este reglamento.

3. En todo caso, la Agencia Española de Protección de Datos dará publicidad a los códigos tipo inscritos, preferentemente a través de medios informáticos o telemáticos.

Artículo 78. *Obligaciones posteriores a la inscripción del código tipo.*

Las entidades promotoras o los órganos, personas o entidades que al efecto se designen en el propio código tipo tendrán, una vez el mismo haya sido publicado, las siguientes obligaciones:

a) Mantener accesible al público la información actualizada sobre las entidades promotoras, el contenido del código tipo, los procedimientos de adhesión y de garantía de su cumplimiento y la relación de adheridos a la que se refiere el artículo anterior.

Esta información deberá presentarse de forma concisa y clara y estar permanentemente accesible por medios electrónicos.

b) Remitir a la Agencia Española de Protección de Datos una memoria anual sobre las actividades realizadas para difundir el código tipo y promover la adhesión a éste, las actuaciones de verificación del cumplimiento del código y sus resultados, las quejas y reclamaciones tramitadas y el curso que se les hubiera dado y cualquier otro aspecto que las entidades promotoras consideren adecuado destacar.

Cuando se trate de códigos tipo inscritos en el registro de una autoridad de control de una comunidad autónoma, la remisión se realizará a dicha autoridad, que dará traslado al registro General de Protección de Datos.

c) Evaluar periódicamente la eficacia del código tipo, midiendo el grado de satisfacción de los afectados y, en su caso, actualizar su contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento.

Esta evaluación deberá tener lugar, al menos, cada cuatro años, salvo que sea precisa la adaptación de los compromisos del código a la modificación de la normativa aplicable en un plazo menor.

d) Favorecer la accesibilidad de todas las personas, con especial atención a las que tengan alguna discapacidad o de edad avanzada a toda la información disponible sobre el código tipo.

TÍTULO VIII

De las medidas de seguridad en el tratamiento de datos de carácter personal

CAPÍTULO I

Disposiciones generales

Artículo 79. *Alcance.*

Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento.

Artículo 80. *Niveles de seguridad.*

Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.

Artículo 81. *Aplicación de los niveles de seguridad.*

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquéllos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.

b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Artículo 82. *Encargado del tratamiento.*

1. Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

Cuando dicho acceso sea remoto habiéndose prohibido al encargado incorporar tales datos a sistemas o soportes distintos de los del responsable, este último deberá hacer constar esta circunstancia en el documento de seguridad del responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

2. Si el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad en los términos exigidos por el artículo 88 de este reglamento o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

3. En todo caso, el acceso a los datos por el encargado del tratamiento estará sometido a las medidas de seguridad contempladas en este reglamento.

Artículo 83. *Prestaciones de servicios sin acceso a datos personales.*

El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos

del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.

Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.

Artículo 84. *Delegación de autorizaciones.*

Las autorizaciones que en este título se atribuyen al responsable del fichero o tratamiento podrán ser delegadas en las personas designadas al efecto. En el documento de seguridad deberán constar las personas habilitadas para otorgar estas autorizaciones así como aquellas en las que recae dicha delegación. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.

Artículo 85. *Acceso a datos a través de redes de comunicaciones.*

Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.

Artículo 86. *Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.*

1. Cuando los datos personales se almacenen en dispositivos portátiles o se traten fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento será preciso que exista una autorización previa del responsable del fichero o tratamiento, y en todo caso deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

2. La autorización a la que se refiere el párrafo anterior tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Artículo 87. *Ficheros temporales o copias de trabajo de documentos.*

1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.

2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

CAPÍTULO II

Del documento de seguridad

Artículo 88. *El documento de seguridad.*

1. El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CAPÍTULO III

Medidas de seguridad aplicables a ficheros y tratamientos automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 89. *Funciones y obligaciones del personal.*

1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Artículo 90. *Registro de incidencias.*

Deberá existir un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas.

Artículo 91. *Control de acceso.*

1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

Artículo 92. *Gestión de soportes y documentos.*

1. Los soportes y documentos que contengan datos de carácter personal deberán permitir identificar el tipo de información que contienen, ser inventariados y solo deberán ser accesibles por el personal autorizado para ello en el documento de seguridad.

Se exceptúan estas obligaciones cuando las características físicas del soporte imposibiliten su cumplimiento, quedando constancia motivada de ello en el documento de seguridad.

2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.
3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

Artículo 93. *Identificación y autenticación.*

1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.
2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

4. El documento de seguridad establecerá la periodicidad, que en ningún caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Artículo 94. *Copias de respaldo y recuperación.*

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 95. *Responsable de seguridad.*

En el documento de seguridad deberán designarse uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

Artículo 96. *Auditoría.*

1. A partir del nivel medio los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen modificaciones sustanciales en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas. Esta auditoría inicia el cómputo de dos años señalado en el párrafo anterior.

2. El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y las recomendaciones propuestas.

3. Los informes de auditoría serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del fichero o tratamiento para que adopte las medidas correctoras adecuadas y quedarán a disposición de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las comunidades autónomas.

Artículo 97. *Gestión de soportes y documentos.*

1. Deberá establecerse un sistema de registro de entrada de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

2. Igualmente, se dispondrá de un sistema de registro de salida de soportes que permita, directa o indirectamente, conocer el tipo de documento o soporte, la fecha y hora, el destinatario, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.

Artículo 98. *Identificación y autenticación.*

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Artículo 99. *Control de acceso físico.*

Exclusivamente el personal autorizado en el documento de seguridad podrá tener acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

Artículo 100. *Registro de incidencias.*

1. En el registro regulado en el artículo 90 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

2. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 101. *Gestión y distribución de soportes.*

1. La identificación de los soportes se deberá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

2. La distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando otro mecanismo que garantice que dicha información no sea accesible o manipulada durante su transporte.

Asimismo, se cifrarán los datos que contengan los dispositivos portátiles cuando éstos se encuentren fuera de las instalaciones que están bajo el control del responsable del fichero.

3. Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. En caso de que sea estrictamente necesario se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

Artículo 102. *Copias de respaldo y recuperación.*

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar diferente de aquel en que se encuentren los equipos

informáticos que los tratan, que deberá cumplir en todo caso las medidas de seguridad exigidas en este título, o utilizando elementos que garanticen la integridad y recuperación de la información, de forma que sea posible su recuperación.

Artículo 103. *Registro de accesos.*

1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Artículo 104. *Telecomunicaciones.*

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

CAPÍTULO IV

Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados

Sección 1.ª Medidas de seguridad de nivel básico

Artículo 105. *Obligaciones comunes.*

1. Además de lo dispuesto en el presente capítulo, a los ficheros no automatizados les será de aplicación lo dispuesto en los capítulos I y II del presente título en lo relativo a:

a) Alcance.
b) Niveles de seguridad.
c) Encargado del tratamiento.
d) Prestaciones de servicios sin acceso a datos personales.
e) Delegación de autorizaciones.
f) Régimen de trabajo fuera de los locales del responsable del fichero o encargado del tratamiento.
g) Copias de trabajo de documentos.
h) Documento de seguridad.

2. Asimismo se les aplicará lo establecido por la sección primera del capítulo III del presente título en lo relativo a:
a) Funciones y obligaciones del personal.

b) Registro de incidencias.
c) Control de acceso.
d) Gestión de soportes.

Artículo 106. *Criterios de archivo.*

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación. Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y consulta de la información y posibilitar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.

En aquellos casos en los que no exista norma aplicable, el responsable del fichero deberá establecer los criterios y procedimientos de actuación que deban seguirse para el archivo.

Artículo 107. *Dispositivos de almacenamiento.*

Los dispositivos de almacenamiento de los documentos que contengan datos de carácter personal deberán disponer de mecanismos que obstaculicen su apertura. Cuando las características físicas de aquéllos no permitan adoptar esta medida, el responsable del fichero o tratamiento adoptará medidas que impidan el acceso de personas no autorizadas.

Artículo 108. *Custodia de los soportes.*

Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecidos en el artículo anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

Sección 2.ª Medidas de seguridad de nivel medio

Artículo 109. *Responsable de seguridad.*

Se designará uno o varios responsables de seguridad en los términos y con las funciones previstas en el artículo 95 de este reglamento.

Artículo 110. *Auditoría.*

Los ficheros comprendidos en la presente sección se someterán, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título.

Sección 3.ª Medidas de seguridad de nivel alto

Artículo 111. *Almacenamiento de la información.*

1. Los armarios, archivadores u otros elementos en los que se almacenen los ficheros no automatizados con datos de carácter personal deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso dotadas de sistemas de apertura mediante llave u otro dispositivo equivalente. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en el fichero.

2. Si, atendidas las características de los locales de que dispusiera el responsable del fichero o tratamiento, no fuera posible cumplir lo establecido en el apartado anterior, el responsable adoptará medidas alternativas que, debidamente motivadas, se incluirán en el documento de seguridad.

Artículo 112. *Copia o reproducción.*

1. La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.

2. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

Artículo 113. *Acceso a la documentación.*

1. El acceso a la documentación se limitará exclusivamente al personal autorizado.
2. Se establecerán mecanismos que permitan identificar los accesos realizados en el caso de documentos que puedan ser utilizados por múltiples usuarios.
3. El acceso de personas no incluidas en el párrafo anterior deberá quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Artículo 114. *Traslado de documentación.*

Siempre que se proceda al traslado físico de la documentación contenida en un fichero, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado.

TÍTULO IX

Procedimientos tramitados por la Agencia Española de Protección de Datos

CAPÍTULO I

Disposiciones generales

Artículo 115. *Régimen aplicable.*

1. Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el presente título, y supletoriamente, por la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
2. Específicamente serán de aplicación las normas reguladoras del procedimiento administrativo común al régimen de representación en los citados procedimientos.

Artículo 116. *Publicidad de las resoluciones.*

1. La Agencia Española de Protección de Datos hará públicas sus resoluciones, con excepción de las correspondientes a la inscripción de un fichero o tratamiento en el Registro General de Protección de Datos y de aquéllas por las que se resuelva la inscripción en el mismo de los códigos tipo, siempre que se refieran a procedimientos que se hubieran iniciado con posterioridad al 1 de enero de 2004, o correspondan al archivo de actuaciones inspectoras incoadas a partir de dicha fecha.
2. La publicación de estas resoluciones se realizará preferentemente mediante su inserción en el sitio web de la Agencia Española de Protección de Datos, dentro del plazo de un mes a contar desde la fecha de su notificación a los interesados.
3. En la notificación de las resoluciones se informará expresamente a los interesados de la publicidad prevista en el artículo 37.2 de la Ley Orgánica 15/1999, de 13 de diciembre.
4. La publicación se realizará aplicando los criterios de disociación de los datos de carácter personal que a tal efecto se establezcan mediante Resolución del Director de la Agencia.

CAPÍTULO II

Procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición

Artículo 117. *Instrucción del procedimiento.*

1. El procedimiento se iniciará a instancia del afectado o afectados, expresando con claridad el contenido de su reclamación y de los preceptos de la Ley Orgánica 15/1999, de 13 de diciembre, que se consideran vulnerados.

2. Recibida la reclamación en la Agencia Española de Protección de Datos, se dará traslado de la misma al responsable del fichero, para que, en el plazo de quince días, formule las alegaciones que estime pertinentes.

3. Recibidas las alegaciones o transcurrido el plazo previsto en el apartado anterior, la Agencia Española de Protección de Datos, previos los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Artículo 118. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento de tutela de derechos será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la reclamación del afectado o afectados.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su reclamación por silencio administrativo positivo.

Artículo 119. *Ejecución de la resolución.*

Si la resolución de tutela fuese estimatoria, se requerirá al responsable del fichero para que, en el plazo de diez días siguientes a la notificación, haga efectivo el ejercicio de los derechos objeto de la tutela, debiendo dar cuenta por escrito de dicho cumplimiento a la Agencia Española de Protección de Datos en idéntico plazo.

CAPÍTULO III

Procedimientos relativos al ejercicio de la potestad sancionadora

Sección 1.ª Disposiciones generales

Artículo 120. *Ámbito de aplicación.*

1. Las disposiciones contenidas en el presente capítulo serán de aplicación a los procedimientos relativos al ejercicio por la Agencia Española de Protección de Datos de la potestad sancionadora que le viene atribuida por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, en la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico, y en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

2. No obstante, las disposiciones previstas en el ar-tículo 121 y en la sección cuarta de este capítulo únicamente serán aplicables a los procedimientos referidos al ejercicio de la potestad sancionadora prevista en la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 121. *Inmovilización de ficheros.*

1. En el supuesto previsto como infracción muy grave en la Ley Orgánica 15/1999, de 13 de diciembre, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia Española de Protección de Datos podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos.

2. El requerimiento deberá ser atendido en el plazo improrrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que tenga por convenientes en orden al levantamiento de la medida.

3. Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

Sección 2.ª Actuaciones previas

Artículo 122. *Iniciación.*

1. Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

2. Las actuaciones previas se llevarán a cabo de oficio por la Agencia Española de Protección de Datos, bien por iniciativa propia o como consecuencia de la existencia de una denuncia o una petición razonada de otro órgano.

3. Cuando las actuaciones se lleven a cabo como consecuencia de la existencia de una denuncia o de una petición razonada de otro órgano, la Agencia Española de Protección de Datos acusará recibo de la denuncia o petición, pudiendo solicitar cuanta documentación se estime oportuna para poder comprobar los hechos susceptibles de motivar la incoación del procedimiento sancionador.

4. Estas actuaciones previas tendrán una duración máxima de doce meses a contar desde la fecha en la que la denuncia o petición razonada a las que se refiere el apartado 2 hubieran tenido entrada en la Agencia Española de Protección de Datos o, en caso de no existir aquéllas, desde que el Director de la Agencia acordase la realización de dichas actuaciones.

El vencimiento del plazo sin que haya sido dictado y notificado acuerdo de inicio de procedimiento sancionador producirá la caducidad de las actuaciones previas.

Artículo 123. *Personal competente para la realización de las actuaciones previas.*

1. Las actuaciones previas serán llevadas a cabo por el personal del área de la Inspección de Datos habilitado para el ejercicio de funciones inspectoras.

2. **(Anulado)**

3. Los funcionarios que ejerzan la inspección a los que se refieren los dos apartados anteriores tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 124. *Obtención de información.*

Los inspectores podrán recabar cuantas informaciones precisen para el cumplimiento de sus cometidos. A tal fin podrán requerir la exhibición o el envío de los documentos y datos y examinarlos en el lugar en que se encuentren depositados, como obtener copia de los mismos, inspeccionar los equipos físicos y lógicos, así como requerir la ejecución de tratamientos y programas o procedimientos de gestión y soporte del fichero o ficheros sujetos a investigación, accediendo a los lugares donde se hallen instalados.

Artículo 125. *Actuaciones presenciales.*

1. En el desarrollo de las actuaciones previas se podrán realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros, en su caso. A tal efecto, los inspectores habrán sido previamente autorizados por el Director de la Agencia Española de Protección de Datos.

Las inspecciones podrán realizarse en el domicilio del inspeccionado, en la sede o local concreto relacionado con el mismo o en cualquiera de sus locales, incluyendo aquéllos en que el tratamiento sea llevado a cabo por un encargado.

La autorización se limitará a indicar la habilitación del inspector autorizado y la identificación de la persona u órgano inspeccionado.

2. En el supuesto contemplado en el apartado anterior, las inspecciones concluirán con el levantamiento de la correspondiente acta, en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de inspección.

3. El acta, que se emitirá por duplicado, será firmada por los inspectores actuantes y por el inspeccionado, que podrá hacer constar en la misma las alegaciones o manifestaciones que tenga por conveniente.

En caso de negativa del inspeccionado a la firma del acta, se hará constar expresamente esta circunstancia en la misma. En todo caso, la firma por el inspeccionado del acta no supondrá su conformidad, sino tan sólo la recepción de la misma.

Se entregará al inspeccionado uno de los originales del acta de inspección, incorporándose el otro a las actuaciones.

Artículo 126. *Resultado de las actuaciones previas.*

1. Finalizadas las actuaciones previas, éstas se someterán a la decisión del Director de la Agencia Española de Protección de Datos.

Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso.

2. En caso de apreciarse la existencia de indicios susceptibles de motivar la imputación de una infracción, el Director de la Agencia Española de Protección de Datos dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas, que se tramitarán conforme a lo dispuesto, respectivamente, en las secciones tercera y cuarta del presente capítulo.

Sección 3.ª Procedimiento sancionador

Artículo 127. *Iniciación del procedimiento.*

Con carácter específico el acuerdo de inicio del procedimiento sancionador deberá contener:

a) Identificación de la persona o personas presuntamente responsables.

b) Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.

d) Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.

e) Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.

f) Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.

g) Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

Artículo 128. *Plazo máximo para resolver.*

1. El plazo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación.

2. El vencimiento del citado plazo máximo, sin que se haya dictada y notificada resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones.

Sección 4.ª Procedimiento de declaración de infracción de la Ley Orgánica 15/1999, de 13 de diciembre, por las administraciones públicas

Artículo 129. *Disposición general.*

El procedimiento por el que se declare la existencia de una infracción de la Ley Orgánica 15/1999, de 13 de diciembre, cometida por las Administraciones públicas será el establecido en la sección tercera de este capítulo.

CAPÍTULO IV

Procedimientos relacionados con la inscripción o cancelación de ficheros

Sección 1.ª Procedimiento de inscripción de la creación, modificación o supresión de ficheros

Artículo 130. *Iniciación del procedimiento.*

1. El procedimiento se iniciará como consecuencia de la notificación de la creación, modificación o supresión del fichero por el interesado o, en su caso, de la comunicación efectuada por las autoridades de control de las comunidades autónomas, a la que se refiere el presente reglamento.

2. La notificación se deberá efectuar cumplimentando los modelos o formularios electrónicos publicados al efecto por la Agencia Española de Protección de Datos, en virtud de lo dispuesto en el apartado 1 del artículo 59 de este reglamento.

Tratándose de la notificación de la modificación o supresión de un fichero, deberá indicarse en la misma el código de inscripción del fichero en el Registro General de Protección de Datos.

3. La notificación se efectuará en soporte electrónico, ya mediante comunicación electrónica a través de Internet mediante firma electrónica o en soporte informático, utilizando al efecto el programa de ayuda para la generación de notificaciones que la Agencia pondrá a disposición de los interesados de forma gratuita.

Será igualmente válida la notificación efectuada en soporte papel cuando para su cumplimentación hayan sido utilizados los modelos o formularios publicados por la Agencia.

4. En la notificación, el responsable del fichero deberá declarar un domicilio a efectos de notificaciones en el procedimiento.

Artículo 131. *Especialidades en la notificación de ficheros de titularidad pública.*

1. Cuando se trate de la notificación de ficheros de titularidad pública, deberá acompañarse a la notificación una copia de la norma o acuerdo de creación, modificación o supresión del fichero a que hace referencia el ar-tículo 52 del presente reglamento.

Cuando el diario oficial en el que se encuentre publicada la citada norma o acuerdo sea accesible a través de Internet, bastará con indicar en la notificación la dirección electrónica que permita su concreta localización.

2. Recibida la notificación, si la misma no contuviera la información preceptiva o se advirtieran defectos formales, el Registro General de Protección de Datos requerirá al responsable del fichero para que complete o subsane la notificación. El plazo para la subsanación o mejora de la solicitud será de tres meses, en el caso de que se precise la modificación de la norma o acuerdo de creación del fichero.

Artículo 132. *Acuerdo de inscripción o cancelación.*

Si la notificación referida a la creación, modificación o supresión del fichero contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción, la modificación de la inscripción del fichero o la cancelación de la inscripción correspondiente.

Artículo 133. *Improcedencia o denegación de la inscripción.*

El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción, modificación o cancelación cuando de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre.

La resolución será debidamente motivada, con indicación expresa de las causas que impiden la inscripción, modificación o cancelación.

Artículo 134. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución acerca de la inscripción, modificación o cancelación será de un mes.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.

Sección 2.ª Procedimiento de cancelación de oficio de ficheros inscritos

Artículo 135. *Iniciación del procedimiento.*

El procedimiento de cancelación de oficio de los ficheros inscritos en el Registro General de Protección de Datos se iniciará siempre de oficio, bien por propia iniciativa o en virtud de denuncia, por acuerdo del Director de la Agencia Española de Protección de Datos.

Artículo 136. *Terminación del expediente.*

La resolución, previa audiencia del interesado, acordará haber lugar o no a la cancelación del fichero.

Si la resolución acordase la cancelación del fichero, se dará traslado de la misma al Registro General de Protección de Datos, para que proceda a la cancelación.

CAPÍTULO V

Procedimientos relacionados con las transferencias internacionales de datos

Sección 1.ª Procedimiento de autorización de transferencias internacionales de datos

Artículo 137. *Iniciación del procedimiento.*

1. El procedimiento para la obtención de la autorización para las transferencias internacionales de datos a países terceros a las que se refiere el artículo 33 de la Ley Orgánica 15/1999, de 13 de diciembre, y el artículo 70 de este reglamento se iniciará siempre a solicitud del exportador que pretenda llevar a cabo la transferencia.

2. En su solicitud, además de los requisitos legalmente exigidos, el exportador deberá consignar, en todo caso:

a) La identificación del fichero o ficheros a cuyos datos se refiera la transferencia internacional, con indicación de su denominación y código de inscripción del fichero en el Registro General de Protección de Datos.

b) La transferencia o transferencias respecto de las que se solicita la autorización, con indicación de la finalidad que la justifica.

c) La documentación que incorpore las garantías exigibles para la obtención de la autorización así como el cumplimiento de los requisitos legales necesarios para la realización de la transferencia, en su caso.

Cuando la autorización se fundamente en la existencia de un contrato entre el exportador y el importador de los datos, deberá aportarse copia del mismo, acreditándose asimismo la concurrencia de poder suficiente en sus otorgantes.

Si la autorización se pretendiera fundar en lo dispuesto en el apartado 4 del artículo 70, deberán aportarse las normas o reglas adoptadas en relación con el tratamiento de los datos en el seno del grupo, así como la documentación que acredite su carácter vinculante y su eficacia dentro del grupo. Igualmente deberá aportarse la documentación que acredite la posibilidad de que el afectado o la Agencia Española de Protección de Datos puedan exigir la responsabilidad que corresponda en caso de perjuicio del afectado o vulneración de las normas de protección de datos por parte de cualquier empresa importadora.

Artículo 138. *Instrucción del procedimiento.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un

período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha Ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

3. Transcurrido el plazo previsto en el apartado 1, en caso de que se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 139. *Actos posteriores a la resolución.*

1. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la transferencia internacional de datos, se dará traslado de la resolución de autorización al Registro General de Protección de Datos, a fin de proceder a su inscripción.

El Registro General de Protección de Datos inscribirá de oficio la autorización de transferencia internacional.

2. En todo caso, se dará traslado de la resolución de autorización o denegación de la autorización de la transferencia internacional de datos al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 140. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá autorizada la transferencia internacional de datos.

Sección 2.ª Procedimiento de suspensión temporal de transferencias internacionales de datos

Artículo 141. *Iniciación.*

1. En los supuestos contemplados en el artículo 69 y en el apartado 3 del artículo 70, el Director de la Agencia Española de Protección de Datos podrá acordar la suspensión temporal de una transferencia internacional de datos.

2. En tales supuestos, el Director dictará acuerdo de inicio referido a la suspensión temporal de la transferencia. El acuerdo deberá ser motivado y fundarse en los supuestos previstos en este reglamento.

Artículo 142. *Instrucción y resolución.*

1. Se dará traslado del acuerdo al exportador, a fin de que en el plazo de quince días formule lo que a su derecho convenga.

2. Recibidas las alegaciones o cumplido el plazo señalado, el Director dictará resolución acordando, en su caso, la suspensión temporal de la transferencia internacional de datos.

Artículo 143. *Actos posteriores a la resolución.*

1. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el registro.

El Registro General de Protección de Datos inscribirá de oficio la suspensión temporal de la transferencia internacional.

2. En todo caso, se dará traslado de la resolución al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26.3 de la Directiva 95/46/CE.

Artículo 144. *Levantamiento de la suspensión temporal.*

1. La suspensión se levantará tan pronto como cesen las causas que la hubieran justificado, mediante resolución del Director de la Agencia Española de Protección de Datos, del que se dará traslado al exportador.

2. El Director de la Agencia Española de Protección de Datos dará traslado de la resolución al Registro General de Protección de Datos, a fin de que la misma se haga constar en el Registro.

El Registro General de Protección de Datos hará constar de oficio el levantamiento de la suspensión temporal de la transferencia internacional.

3. El acuerdo será notificado al exportador y al Ministerio de Justicia, al efecto de que se proceda a su notificación a la Comisión Europea y a los demás Estados miembros de la Unión Europea de acuerdo a lo previsto en el artículo 26. 3 de la Directiva 95/46/CE.

CAPÍTULO VI

Procedimiento de inscripción de códigos tipo

Artículo 145. *Iniciación del procedimiento.*

1. El procedimiento para la inscripción en el Registro General de Protección de Datos de los códigos tipo se iniciará siempre a solicitud de la entidad, órgano o asociación promotora del código tipo.

2. La solicitud, que deberá reunir los requisitos legalmente establecidos, habrá de acompañarse de los siguientes documentos:

a) Acreditación de la representación que concurra en la persona que presente la solicitud.

b) Contenido del acuerdo, convenio o decisión por la que se aprueba, en el ámbito correspondiente el contenido del código tipo presentado.

c) En caso de que el código tipo proceda de un acuerdo sectorial o una decisión de empresa certificación referida a la adopción del acuerdo y legitimación del órgano que lo adoptó.

d) En el supuesto contemplado en la letra anterior, copia de los estatutos de la asociación, organización sectorial o entidad en cuyo marco haya sido aprobado el código.

e) En caso de códigos tipo presentados por asociaciones u organizaciones de carácter sectorial, documentación relativa a su representatividad en el sector.

f) En caso de códigos tipo basados en decisiones de empresa, descripción de los tratamientos a los que se refiere el código tipo.

g) Código tipo sometido a la Agencia Española de Protección de Datos.

Artículo 146. *Análisis de los aspectos sustantivos del código tipo.*

1. Durante los treinta días siguientes a la notificación o subsanación de los defectos el Registro General de Protección de Datos podrá convocar a los solicitantes, a fin de obtener aclaraciones o precisiones relativas al contenido sustantivo del código tipo.

2. Transcurrido el plazo señalado en el apartado anterior, el Registro General de Protección de Datos elaborará un informe sobre las características del proyecto de código tipo.

3. La documentación presentada y el informe del Registro serán remitidos al Gabinete Jurídico, a fin de que por el mismo se informe acerca del cumplimiento de los requisitos establecidos en el Título VII de este Reglamento.

Artículo 147. *Información pública.*

1. Cuando el Director de la Agencia Española de Protección de Datos acuerde, conforme a lo dispuesto en el artículo 86.1 de la Ley 30/1992, de 26 de noviembre, la apertura de un período de información pública, el plazo para la formulación de alegaciones será de diez días a contar desde la publicación en el «Boletín Oficial del Estado» del anuncio previsto en dicha ley.

2. No será posible el acceso a la información del expediente en que concurran las circunstancias establecidas en el artículo 37.5 de la Ley 30/1992, de 26 de noviembre.

Artículo 148. *Mejora del código tipo.*

Si durante la tramitación del procedimiento resultase necesaria la aportación de nuevos documentos o la modificación del código tipo presentado, la Agencia Española de Protección de Datos podrá requerir al solicitante, a fin de que en el plazo de treinta días introduzca las modificaciones que sean precisas, remitiendo el texto resultante a la Agencia Española de Protección de Datos.

Se declarará la suspensión del procedimiento en tanto el solicitante no dé cumplimiento al requerimiento.

Artículo 149. *Trámite de audiencia.*

En caso de que durante el trámite previsto en el ar-tículo 148 se hubieran formulado alegaciones, se dará traslado de las mismas al solicitante de la autorización, a fin de que en el plazo de diez días alegue lo que estime procedente.

Artículo 150. *Resolución.*

1. Cumplidos los términos establecidos en los artículos precedentes, el Director de la Agencia resolverá sobre la procedencia o improcedencia de la inscripción del código tipo en el Registro General de Protección de Datos.

2. Cuando el Director de la Agencia Española de Protección de Datos resuelva autorizar la inscripción del código tipo, se dará traslado de la resolución al Registro General de Protección de Datos, a fin de proceder a su inscripción.

Artículo 151. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución será de seis meses, a contar desde la fecha de entrada de la solicitud en la Agencia Española de Protección de Datos.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el solicitante podrá considerar estimada su solicitud.

Artículo 152. *Publicación de los códigos tipo por la Agencia Española de Protección de Datos.*

La Agencia Española de Protección de Datos dará publicidad al contenido de los códigos tipo inscritos en el Registro General de Protección de Datos, utilizando para ello, con carácter preferente, medios electrónicos o telemáticos.

CAPÍTULO VII

Otros procedimientos tramitados por la agencia española de protección de datos

Sección 1.ª Procedimiento de exención del deber de información al interesado

Artículo 153. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la exención del deber de informar al interesado acerca del tratamiento de sus datos de carácter personal cuando resulte imposible o exija esfuerzos desproporcionados, prevista en el apartado 5 del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, se iniciará siempre a petición del responsable que pretenda obtener la aplicación de la exención.

2. En el escrito de solicitud, además de los requisitos recogidos en el art. 70 de la Ley 30/1992, de 26 de noviembre, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la exención del deber de informar.

b) Motivar expresamente las causas en que fundamenta la imposibilidad o el carácter desproporcionado del esfuerzo que implicaría el cumplimiento del deber de informar.

c) Exponer detalladamente las medidas compensatorias que propone realizar en caso de exoneración del cumplimiento del deber de informar.

d) Aportar una cláusula informativa que, mediante su difusión, en los términos que se indiquen en la solicitud, permita compensar la exención del deber de informar.

Artículo 154. *Propuesta de nuevas medidas compensatorias.*

1. Si la Agencia Española de Protección de Datos considerase insuficientes las medidas compensatorias propuestas por el solicitante, podrá acordar la adopción de medidas complementarias o sustitutivas a las propuestas por aquél en su solicitud.

2. Del acuerdo se dará traslado al solicitante, a fin de que exponga lo que a su derecho convenga en el plazo de quince días.

Artículo 155. *Terminación del procedimiento.*

Concluidos los trámites previstos en los artículos precedentes, el Director de la Agencia dictará resolución, concediendo o denegando la exención del deber de informar. La resolución podrá imponer la adopción de las medidas complementarias a las que se refiere el artículo anterior.

Artículo 156. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de seis meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud por silencio administrativo positivo.

Sección 2.ª Procedimiento para la autorización de conservación de datos para fines históricos, estadísticos o científicos

Artículo 157. *Iniciación del procedimiento.*

1. El procedimiento para obtener de la Agencia Española de Protección de Datos la declaración de la concurrencia en un determinado tratamiento de datos de valores históricos, científicos o estadísticos, a los efectos previstos en la Ley Orgánica 15/1999, de 13 de diciembre, y en el presente Reglamento, se iniciará siempre a petición del responsable que pretenda obtener la declaración.

2. En el escrito de solicitud, el responsable deberá:

a) Identificar claramente el tratamiento de datos al que pretende aplicarse la excepción.

b) Motivar expresamente las causas que justificarían la declaración.

c) Exponer detalladamente las medidas que el responsable del fichero se propone implantar para garantizar el derecho de los ciudadanos.

3. La solicitud deberá acompañarse de cuantos documentos o pruebas sean necesarios para justificar la existencia de los valores históricos, científicos o estadísticos que fundamentarían la declaración de la Agencia.

Artículo 158. *Duración del procedimiento y efectos de la falta de resolución expresa.*

1. El plazo máximo para dictar y notificar resolución en el procedimiento será de tres meses, a contar desde la fecha de entrada en la Agencia Española de Protección de Datos de la solicitud del responsable del fichero.

2. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, el afectado podrá considerar estimada su solicitud.

Disposición adicional única. *Productos de software.*

Los productos de software destinados al tratamiento automatizado de datos personales deberán incluir en su descripción técnica el nivel de seguridad, básico, medio o alto, que permitan alcanzar de acuerdo con lo establecido en el título VIII de este reglamento.

Disposición final única. *Aplicación supletoria.*

En lo no establecido en el capítulo III del título IX serán de aplicación a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos las disposiciones contenidas en el Reglamento del Procedimiento para el ejercicio de la potestad sancionadora, aprobado por Real Decreto 1398/1993, de 4 de agosto.

§ 64

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

Unión Europea
«DOUE» núm. 119, de 4 de mayo de 2016
Última modificación: sin modificaciones
Referencia: DOUE-L-2016-89807

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea, y en particular su artículo 16,

Vista la propuesta de la Comisión Europea,

Previa transmisión del proyecto de texto legislativo a los Parlamentos nacionales,

Visto el dictamen del Comité Económico y Social Europeo [1],

Visto el dictamen del Comité de las Regiones [2],

De conformidad con el procedimiento legislativo ordinario [3],

Considerando lo siguiente:

(1) La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea («la Carta») y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

(2) Los principios y normas relativos a la protección de las personas físicas en lo que respecta al tratamiento de sus datos de carácter personal deben, cualquiera que sea su nacionalidad o residencia, respetar sus libertades y derechos fundamentales, en particular el derecho a la protección de los datos de carácter personal. El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas.

(3) La Directiva 95/46/CE del Parlamento Europeo y del Consejo [4] trata de armonizar la protección de los derechos y las libertades fundamentales de las personas físicas en relación con las actividades de tratamiento de datos de carácter personal y garantizar la libre circulación de estos datos entre los Estados miembros.

(4) El tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe

considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad. El presente Reglamento respeta todos los derechos fundamentales y observa las libertades y los principios reconocidos en la Carta conforme se consagran en los Tratados, en particular el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística.

(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(7) Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas.

(8) En los casos en que el presente Reglamento establece que sus normas sean especificadas o restringidas por el Derecho de los Estados miembros, estos, en la medida en que sea necesario por razones de coherencia y para que las disposiciones nacionales sean comprensibles para sus destinatarios, pueden incorporar a su Derecho nacional elementos del presente Reglamento.

(9) Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE.

(10) Para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogénea. En lo que respecta al tratamiento de datos personales para el cumplimiento de una obligación legal, para el cumplimiento de una misión

realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los Estados miembros deben estar facultados para mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento. Junto con la normativa general y horizontal sobre protección de datos por la que se aplica la Directiva 95/46/CE, los Estados miembros cuentan con distintas normas sectoriales específicas en ámbitos que precisan disposiciones más específicas. El presente Reglamento reconoce también un margen de maniobra para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales («datos sensibles»). En este sentido, el presente Reglamento no excluye el Derecho de los Estados miembros que determina las circunstancias relativas a situaciones específicas de tratamiento, incluida la indicación pormenorizada de las condiciones en las que el tratamiento de datos personales es lícito.

(11) La protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes.

(12) El artículo 16, apartado 2, del TFUE encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos.

(13) Para garantizar un nivel coherente de protección de las personas físicas en toda la Unión y evitar divergencias que dificulten la libre circulación de datos personales dentro del mercado interior, es necesario un reglamento que proporcione seguridad jurídica y transparencia a los operadores económicos, incluidas las microempresas y las pequeñas y medianas empresas, y ofrezca a las personas físicas de todos los Estados miembros el mismo nivel de derechos y obligaciones exigibles y de responsabilidades para los responsables y encargados del tratamiento, con el fin de garantizar una supervisión coherente del tratamiento de datos personales y sanciones equivalentes en todos los Estados miembros, así como la cooperación efectiva entre las autoridades de control de los diferentes Estados miembros. El buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales. Con objeto de tener en cuenta la situación específica de las microempresas y las pequeñas y medianas empresas, el presente Reglamento incluye una serie de excepciones en materia de llevanza de registros para organizaciones con menos de 250 empleados. Además, alienta a las instituciones y órganos de la Unión y a los Estados miembros y a sus autoridades de control a tener en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas en la aplicación del presente Reglamento. El concepto de microempresas y pequeñas y medianas empresas debe extraerse del artículo 2 del anexo de la Recomendación 2003/361/CE de la Comisión [(5)].

(14) La protección otorgada por el presente Reglamento debe aplicarse a las personas físicas, independientemente de su nacionalidad o de su lugar de residencia, en relación con el tratamiento de sus datos personales. El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto.

(15) A fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del presente Reglamento.

(16) El presente Reglamento no se aplica a cuestiones de protección de los derechos y las libertades fundamentales o la libre circulación de datos personales relacionadas con

actividades excluidas del ámbito de del Derecho de la Unión, como las actividades relativas a la seguridad nacional. Tampoco se aplica al tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades relacionadas con la política exterior y de seguridad común de la Unión.

(17) El Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo [6] se aplica al tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal deben adaptarse a los principios y normas establecidos en el presente Reglamento y aplicarse a la luz del mismo. A fin de establecer un marco sólido y coherente en materia de protección de datos en la Unión, una vez adoptado el presente Reglamento deben introducirse las adaptaciones necesarias del Reglamento (CE) n.º 45/2001, con el fin de que pueda aplicarse al mismo tiempo que el presente Reglamento.

(18) El presente Reglamento no se aplica al tratamiento de datos de carácter personal por una persona física en el curso de una actividad exclusivamente personal o doméstica y, por tanto, sin conexión alguna con una actividad profesional o comercial. Entre las actividades personales o domésticas cabe incluir la correspondencia y la llevanza de un repertorio de direcciones, o la actividad en las redes sociales y la actividad en línea realizada en el contexto de las citadas actividades. No obstante, el presente Reglamento se aplica a los responsables o encargados del tratamiento que proporcionen los medios para tratar datos personales relacionados con tales actividades personales o domésticas.

(19) La protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión. El presente Reglamento no debe, por lo tanto, aplicarse a las actividades de tratamiento destinadas a tales fines. No obstante, los datos personales tratados por las autoridades públicas en aplicación del presente Reglamento deben, si se destinan a tales fines, regirse por un acto jurídico de la Unión más específico, concretamente la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo [7]. Los Estados miembros pueden encomendar a las autoridades competentes, tal como se definen en la Directiva (UE) 2016/680, funciones que no se lleven a cabo necesariamente con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o ejecución de sanciones penales, incluida la protección frente a las amenazas a la seguridad pública y su prevención, de tal forma que el tratamiento de datos personales para estos otros fines, en la medida en que esté incluido en el ámbito del Derecho de la Unión, entra en el ámbito de aplicación del presente Reglamento.

En lo que respecta al tratamiento de datos personales por parte de dichas autoridades competentes con fines que entren en el ámbito de aplicación del presente Reglamento, los Estados miembros deben tener la posibilidad de mantener o introducir disposiciones más específicas para adaptar la aplicación de las normas del presente Reglamento. Tales disposiciones pueden establecer de forma más precisa requisitos concretos para el tratamiento de datos personales con otros fines por parte de dichas autoridades competentes, tomando en consideración la estructura constitucional, organizativa y administrativa del Estado miembro en cuestión. Cuando el tratamiento de datos personales por organismos privados entre en el ámbito de aplicación del presente Reglamento, este debe disponer que los Estados miembros puedan, en condiciones específicas, limitar conforme a Derecho determinadas obligaciones y derechos siempre que dicha limitación sea una medida necesaria y proporcionada en una sociedad democrática para proteger intereses específicos importantes, entre ellos la seguridad pública y la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, inclusive la protección frente a las amenazas contra la seguridad pública y su prevención. Esto se aplica, por ejemplo, en el marco de la lucha contra el blanqueo de capitales o de las actividades de los laboratorios de policía científica.

(20) Aunque el presente Reglamento se aplica, entre otras, a las actividades de los tribunales y otras autoridades judiciales, en virtud del Derecho de la Unión o de los Estados

miembros pueden especificarse las operaciones de tratamiento y los procedimientos de tratamiento en relación con el tratamiento de datos personales por los tribunales y otras autoridades judiciales. A fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos.

(21) El presente Reglamento debe entenderse sin perjuicio de la aplicación de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo [8], en particular de las normas en materia de responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15. El objetivo de dicha Directiva es contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros.

(22) Todo tratamiento de datos personales en el contexto de las actividades de un establecimiento de un responsable o un encargado del tratamiento en la Unión debe llevarse a cabo de conformidad con el presente Reglamento, independientemente de que el tratamiento tenga lugar en la Unión. Un establecimiento implica el ejercicio de manera efectiva y real de una actividad a través de modalidades estables. La forma jurídica que revistan tales modalidades, ya sea una sucursal o una filial con personalidad jurídica, no es el factor determinante al respecto.

(23) Con el fin de garantizar que las personas físicas no se vean privadas de la protección a la que tienen derecho en virtud del presente Reglamento, el tratamiento de datos personales de interesados que se encuentran en la Unión por un responsable o un encargado no establecido en la Unión debe regirse por el presente Reglamento si las actividades de tratamiento se refieren a la oferta de bienes o servicios a dichos interesados, independientemente de que medie pago. Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que se encuentran en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión.

(24) El tratamiento de datos personales de los interesados que se encuentran en la Unión por un responsable o encargado no establecido en la Unión debe ser también objeto del presente Reglamento cuando esté relacionado con la observación del comportamiento de dichos interesados en la medida en que este comportamiento tenga lugar en la Unión. Para determinar si se puede considerar que una actividad de tratamiento controla el comportamiento de los interesados, debe evaluarse si las personas físicas son objeto de un seguimiento en internet, inclusive el potencial uso posterior de técnicas de tratamiento de datos personales que consistan en la elaboración de un perfil de una persona física con el fin, en particular, de adoptar decisiones sobre él o de analizar o predecir sus preferencias personales, comportamientos y actitudes.

(25) Cuando sea de aplicación el Derecho de los Estados miembros en virtud del Derecho internacional público, el presente Reglamento debe aplicarse también a todo responsable del tratamiento no establecido en la Unión, como en una misión diplomática u oficina consular de un Estado miembro.

(26) Los principios de la protección de datos deben aplicarse a toda la información relativa a una persona física identificada o identificable. Los datos personales seudonimizados, que cabría atribuir a una persona física mediante la utilización de

información adicional, deben considerarse información sobre una persona física identificable. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física. Para determinar si existe una probabilidad razonable de que se utilicen medios para identificar a una persona física, deben tenerse en cuenta todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Por lo tanto los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación.

(27) El presente Reglamento no se aplica a la protección de datos personales de personas fallecidas. Los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

(28) La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la «seudonimización» en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos.

(29) Para incentivar la aplicación de la seudonimización en el tratamiento de datos personales, debe ser posible establecer medidas de seudonimización, permitiendo al mismo tiempo un análisis general, por parte del mismo responsable del tratamiento, cuando este haya adoptado las medidas técnicas y organizativas necesarias para garantizar que se aplique el presente Reglamento al tratamiento correspondiente y que se mantenga por separado la información adicional para la atribución de los datos personales a una persona concreta. El responsable que trate datos personales debe indicar cuáles son sus personas autorizadas.

(30) Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas.

(31) Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento.

(32) El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las

actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta.

(33) Con frecuencia no es posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida. Por consiguiente, debe permitirse a los interesados dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación o partes de proyectos de investigación, en la medida en que lo permita la finalidad perseguida.

(34) Debe entenderse por datos genéticos los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

(35) Entre los datos personales relativos a la salud se deben incluir todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasado, presente o futuro. Se incluye la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia, de conformidad con la Directiva 2011/24/UE del Parlamento Europeo y del Consejo [9]; todo número, símbolo o dato asignado a una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

(36) El establecimiento principal de un responsable del tratamiento en la Unión debe ser el lugar de su administración central en la Unión, salvo que las decisiones relativas a los fines y medios del tratamiento de los datos personales se tomen en otro establecimiento del responsable en la Unión, en cuyo caso, ese otro establecimiento debe considerarse el establecimiento principal. El establecimiento principal de un responsable en la Unión debe determinarse en función de criterios objetivos y debe implicar el ejercicio efectivo y real de actividades de gestión que determinen las principales decisiones en cuanto a los fines y medios del tratamiento a través de modalidades estables. Dicho criterio no debe depender de si el tratamiento de los datos personales se realiza en dicho lugar. La presencia y utilización de medios técnicos y tecnologías para el tratamiento de datos personales o las actividades de tratamiento no constituyen, en sí mismas, establecimiento principal y no son, por lo tanto, criterios determinantes de un establecimiento principal. El establecimiento principal del encargado del tratamiento debe ser el lugar de su administración central en la Unión o, si careciese de administración central en la Unión, el lugar en el que se llevan a cabo las principales actividades de tratamiento en la Unión. En los casos que impliquen tanto al responsable como al encargado, la autoridad de control principal competente debe seguir siendo la autoridad de control del Estado miembro en el que el responsable tenga su establecimiento principal, pero la autoridad de control del encargado debe considerarse autoridad de control interesada y participar en el procedimiento de cooperación establecido en el presente Reglamento. En cualquier caso, las autoridades de control del Estado miembro o los Estados miembros en los que el encargado tenga uno o varios establecimientos no deben considerarse autoridades de control interesadas cuando el proyecto de decisión afecte únicamente al responsable. Cuando el tratamiento lo realice un grupo empresarial, el establecimiento principal de la empresa que ejerce el control debe considerarse el establecimiento principal del grupo empresarial, excepto cuando los fines y medios del tratamiento los determine otra empresa.

(37) Un grupo empresarial debe estar constituido por una empresa que ejerce el control y las empresas controladas, debiendo ser la empresa que ejerce el control la que pueda ejercer una influencia dominante en las otras empresas, por razones, por ejemplo, de propiedad, participación financiera, normas por las que se rige, o poder de hacer cumplir las normas de protección de datos personales. Una empresa que controle el tratamiento de los datos personales en las empresas que estén afiliadas debe considerarse, junto con dichas empresas, «grupo empresarial».

(38) Los niños merecen una protección específica de sus datos personales, ya que pueden ser menos conscientes de los riesgos, consecuencias, garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y a la obtención de datos personales relativos a niños cuando se utilicen servicios ofrecidos directamente a un niño. El consentimiento del titular de la patria potestad o tutela no debe ser necesario en el contexto de los servicios preventivos o de asesoramiento ofrecidos directamente a los niños.

(39) Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados. El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento.

(40) Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho, ya sea en el presente Reglamento o en virtud de otro Derecho de la Unión o de los Estados miembros a que se refiera el presente Reglamento, incluida la necesidad de cumplir la obligación legal aplicable al responsable del tratamiento o la necesidad de ejecutar un contrato en el que sea parte el interesado o con objeto de tomar medidas a instancia del interesado con anterioridad a la conclusión de un contrato.

(41) Cuando el presente Reglamento hace referencia a una base jurídica o a una medida legislativa, esto no exige necesariamente un acto legislativo adoptado por un parlamento, sin perjuicio de los requisitos de conformidad del ordenamiento constitucional del Estado miembro de que se trate. Sin embargo, dicha base jurídica o medida legislativa debe ser clara y precisa y su aplicación previsible para sus destinatarios, de conformidad con la jurisprudencia del Tribunal de Justicia de la Unión Europea (en lo sucesivo, «Tribunal de Justicia») y del Tribunal Europeo de Derechos Humanos.

(42) Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración

por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo [10], debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.

(43) Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

(44) El tratamiento debe ser lícito cuando sea necesario en el contexto de un contrato o de la intención de concluir un contrato.

(45) Cuando se realice en cumplimiento de una obligación legal aplicable al responsable del tratamiento, o si es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, el tratamiento debe tener una base en el Derecho de la Unión o de los Estados miembros. El presente Reglamento no requiere que cada tratamiento individual se rija por una norma específica. Una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas en una obligación legal aplicable al responsable del tratamiento, o si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos. La finalidad del tratamiento también debe determinase en virtud del Derecho de la Unión o de los Estados miembros. Además, dicha norma podría especificar las condiciones generales del presente Reglamento por las que se rige la licitud del tratamiento de datos personales, establecer especificaciones para la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal. Debe determinarse también en virtud del Derecho de la Unión o de los Estados miembros si el responsable del tratamiento que realiza una misión en interés público o en el ejercicio de poderes públicos debe ser una autoridad pública u otra persona física o jurídica de Derecho público, o, cuando se haga en interés público, incluidos fines sanitarios como la salud pública, la protección social y la gestión de los servicios de sanidad, de Derecho privado, como una asociación profesional.

(46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

(47) El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo,

cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.

(48) Los responsables que forman parte de un grupo empresarial o de entidades afiliadas a un organismo central pueden tener un interés legítimo en transmitir datos personales dentro del grupo empresarial para fines administrativos internos, incluido el tratamiento de datos personales de clientes o empleados. Los principios generales aplicables a la transmisión de datos personales, dentro de un grupo empresarial, a una empresa situada en un país tercero no se ven afectados.

(49) Constituye un interés legítimo del responsable del tratamiento interesado el tratamiento de datos personales en la medida estrictamente necesaria y proporcionada para garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta a incidentes de seguridad informática (CSIRT), proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.

(50) El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición. La indicación de posibles actos delictivos o amenazas para la seguridad pública por parte del responsable del tratamiento y la transmisión a la autoridad competente de los datos respecto de casos individuales o casos diversos relacionados con un mismo acto delictivo o amenaza para la seguridad pública debe considerarse que es en interés legítimo del responsable. Con todo, debe prohibirse esa transmisión en interés legítimo del responsable o el tratamiento ulterior de datos personales si el tratamiento no es compatible con una obligación de secreto legal, profesional o vinculante por otro concepto.

(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.

(52) Asimismo deben autorizarse excepciones a la prohibición de tratar categorías especiales de datos personales cuando lo establezca el Derecho de la Unión o de los Estados miembros y siempre que se den las garantías apropiadas, a fin de proteger datos personales y otros derechos fundamentales, cuando sea en interés público, en particular el tratamiento de datos personales en el ámbito de la legislación laboral, la legislación sobre protección social, incluidas las pensiones y con fines de seguridad, supervisión y alerta sanitaria, la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud. Tal excepción es posible para fines en el ámbito de la salud, incluidas la sanidad pública y la gestión de los servicios de asistencia sanitaria, especialmente con el fin de garantizar la calidad y la rentabilidad de los procedimientos utilizados para resolver las reclamaciones de prestaciones y de servicios en el régimen del seguro de enfermedad, o con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Debe autorizarse asimismo a título excepcional el tratamiento de dichos datos personales cuando sea necesario para la formulación, el ejercicio o la defensa de reclamaciones, ya sea por un procedimiento judicial o un procedimiento administrativo o extrajudicial.

(53) Las categorías especiales de datos personales que merecen mayor protección únicamente deben tratarse con fines relacionados con la salud cuando sea necesario para

lograr dichos fines en beneficio de las personas físicas y de la sociedad en su conjunto, en particular en el contexto de la gestión de los servicios y sistemas sanitarios o de protección social, incluido el tratamiento de esos datos por las autoridades gestoras de la sanidad y las autoridades sanitarias nacionales centrales con fines de control de calidad, gestión de la información y supervisión general nacional y local del sistema sanitario o de protección social, y garantía de la continuidad de la asistencia sanitaria o la protección social y la asistencia sanitaria transfronteriza o fines de seguridad, supervisión y alerta sanitaria, o con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, basados en el Derecho de la Unión o del Estado miembro que ha de cumplir un objetivo de interés público, así como para estudios realizados en interés público en el ámbito de la salud pública. Por tanto, el presente Reglamento debe establecer condiciones armonizadas para el tratamiento de categorías especiales de datos personales relativos a la salud, en relación con necesidades específicas, en particular si el tratamiento de esos datos lo realizan, con fines relacionados con la salud, personas sujetas a la obligación legal de secreto profesional. El Derecho de la Unión o de los Estados miembros debe establecer medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas. Los Estados miembros deben estar facultados para mantener o introducir otras condiciones, incluidas limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud. No obstante, esto no ha de suponer un obstáculo para la libre circulación de datos personales dentro de la Unión cuando tales condiciones se apliquen al tratamiento transfronterizo de esos datos.

(54) El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo [(11)], es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

(55) Se realiza además por razones de interés público el tratamiento de datos personales por las autoridades públicas con el fin de alcanzar los objetivos, establecidos en el Derecho constitucional o en el Derecho internacional público, de asociaciones religiosas reconocidas oficialmente.

(56) Si, en el marco de actividades electorales, el funcionamiento del sistema democrático exige en un Estado miembro que los partidos políticos recopilen datos personales sobre las opiniones políticas de las personas, puede autorizarse el tratamiento de estos datos por razones de interés público, siempre que se ofrezcan garantías adecuadas.

(57) Si los datos personales tratados por un responsable no le permiten identificar a una persona física, el responsable no debe estar obligado a obtener información adicional para identificar al interesado con la única finalidad de cumplir cualquier disposición del presente Reglamento. No obstante, el responsable del tratamiento no debe negarse a recibir información adicional facilitada por el interesado a fin de respaldarle en el ejercicio de sus derechos. La identificación debe incluir la identificación digital de un interesado, por ejemplo mediante un mecanismo de autenticación, como las mismas credenciales, empleadas por el interesado para abrir una sesión en el servicio en línea ofrecido por el responsable.

(58) El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le

conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender.

(59) Deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas.

(60) Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe además informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran. Dicha información puede transmitirse en combinación con unos iconos normalizados que ofrezcan, de forma fácilmente visible, inteligible y claramente legible, una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presentan en formato electrónico deben ser legibles mecánicamente.

(61) Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso. Si los datos personales pueden ser comunicados legítimamente a otro destinatario, se debe informar al interesado en el momento en que se comunican al destinatario por primera vez. El responsable del tratamiento que proyecte tratar los datos para un fin que no sea aquel para el que se recogieron debe proporcionar al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y otra información necesaria. Cuando el origen de los datos personales no pueda facilitarse al interesado por haberse utilizado varias fuentes, debe facilitarse información general.

(62) Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, cuando el registro o la comunicación de los datos personales estén expresamente establecidos por ley, o cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas.

(63) Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan y a ejercer dicho derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento. Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales. Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos. No obstante, estas consideraciones no deben tener

como resultado la negativa a prestar toda la información al interesado. Si trata una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud.

(64) El responsable del tratamiento debe utilizar todas las medidas razonables para verificar la identidad de los interesados que soliciten acceso, en particular en el contexto de los servicios en línea y los identificadores en línea. El responsable no debe conservar datos personales con el único propósito de poder responder a posibles solicitudes.

(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

(66) A fin de reforzar el «derecho al olvido» en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales.

(67) Entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema.

(68) Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al

responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible.

(69) En los casos en que los datos personales puedan ser tratados lícitamente porque el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero, el interesado debe, sin embargo, tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular. Debe ser el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado.

(70) Si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información.

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar, como la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no medie intervención humana alguna. Este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento automatizado de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Sin embargo, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Tal medida no debe afectar a un menor.

A fin de garantizar un tratamiento leal y transparente respecto del interesado, teniendo en cuenta las circunstancias y contexto específicos en los que se tratan los datos personales, el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medidas técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para

los intereses y derechos del interesado e impedir, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o tratamiento que dé lugar a medidas que produzcan tal efecto. Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas.

(72) La elaboración de perfiles está sujeta a las normas del presente Reglamento que rigen el tratamiento de datos personales, como los fundamentos jurídicos del tratamiento o los principios de la protección de datos. El Comité Europeo de Protección de Datos establecido por el presente Reglamento (en lo sucesivo, el «Comité») debe tener la posibilidad de formular orientaciones en este contexto.

(73) El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

(74) Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

(75) Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

(76) La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

(77) Se podrían proporcionar directrices para la aplicación de medidas oportunas y para demostrar el cumplimiento por parte del responsable o del encargado del tratamiento, especialmente con respecto a la identificación del riesgo relacionado con el tratamiento, a su evaluación en términos de origen, naturaleza, probabilidad y gravedad y a la identificación de buenas prácticas para mitigar el riesgo, que revistan, en particular, la forma de códigos de conducta aprobados, certificaciones aprobadas, directrices dadas por el Comité o indicaciones proporcionadas por un delegado de protección de datos. El Comité también puede emitir directrices sobre operaciones de tratamiento que se considere improbable supongan un alto riesgo para los derechos y libertades de las personas físicas, e indicar qué medidas pueden ser suficientes en dichos casos para afrontar el riesgo en cuestión.

(78) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.

(79) La protección de los derechos y libertades de los interesados, así como la responsabilidad de los responsables y encargados del tratamiento, también en lo que respecta a la supervisión por parte de las autoridades de control y a las medidas adoptadas por ellas, requieren una atribución clara de las responsabilidades en virtud del presente Reglamento, incluidos los casos en los que un responsable determine los fines y medios del tratamiento de forma conjunta con otros responsables, o en los que el tratamiento se lleve a cabo por cuenta de un responsable.

(80) El responsable o el encargado del tratamiento no establecido en la Unión que esté tratando datos personales de interesados que se encuentran en la Unión y cuyas actividades de tratamiento están relacionadas con la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si se requiere un pago por parte de estos, o con el control de su comportamiento en la medida en que este tenga lugar en la Unión, debe designar a un representante, a menos que el tratamiento sea ocasional, no incluya el tratamiento a gran escala de categorías especiales de datos personales o el tratamiento de datos personales relativos a condenas e infracciones penales, y sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, vista la naturaleza, el contexto, el ámbito y los fines del tratamiento, o si el responsable del tratamiento es una autoridad u organismo público. El representante debe actuar por cuenta del responsable o el encargado y puede ser contactado por cualquier autoridad de control. El representante debe ser designado expresamente por mandato escrito del responsable o del encargado para que actúe en su nombre con respecto a las obligaciones que les incumben en virtud del presente Reglamento. La designación de dicho representante no afecta a la responsabilidad del responsable o del encargado en virtud del presente Reglamento. Dicho representante debe

desempeñar sus funciones conforme al mandato recibido del responsable o del encargado, incluida la cooperación con las autoridades de control competentes en relación con cualquier medida que se tome para garantizar el cumplimiento del presente Reglamento. El representante designado debe estar sujeto a medidas coercitivas en caso de incumplimiento por parte del responsable o del encargado.

(81) Para garantizar el cumplimiento de las disposiciones del presente Reglamento respecto del tratamiento que lleve a cabo el encargado por cuenta del responsable, este, al encomendar actividades de tratamiento a un encargado, debe recurrir únicamente a encargados que ofrezcan suficientes garantías, en particular en lo que respecta a conocimientos especializados, fiabilidad y recursos, de cara a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento. La adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable. El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento, la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos.

(82) Para demostrar la conformidad con el presente Reglamento, el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad. Todos los responsables y encargados están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, dichos registros, de modo que puedan servir para supervisar las operaciones de tratamiento.

(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales.

(84) A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento.

(85) Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de

sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.

(86) El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

(87) Debe verificarse si se ha aplicado toda la protección tecnológica adecuada y se han tomado las medidas organizativas oportunas para determinar de inmediato si se ha producido una violación de la seguridad de los datos personales y para informar sin dilación a la autoridad de control y al interesado. Debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado. Dicha notificación puede resultar en una intervención de la autoridad de control de conformidad con las funciones y poderes que establece el presente Reglamento.

(88) Al establecer disposiciones de aplicación sobre el formato y los procedimientos aplicables a la notificación de las violaciones de la seguridad de los datos personales, hay que tener debidamente en cuenta las circunstancias de tal violación, inclusive si los datos personales habían sido protegidos mediante las medidas técnicas de protección adecuadas, limitando eficazmente la probabilidad de usurpación de identidad u otras formas de uso indebido. Asimismo, estas normas y procedimientos deben tener en cuenta los intereses legítimos de las autoridades policiales en caso de que una comunicación prematura pueda obstaculizar innecesariamente la investigación de las circunstancias de una violación de la seguridad de los datos personales.

(89) La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales. Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas. Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

(90) En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular

gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

(91) Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados, en particular cuando estas operaciones hace más difícil para los interesados el ejercicio de sus derechos. La evaluación de impacto relativa a la protección de datos debe realizarse también en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz de una evaluación sistemática y exhaustiva de aspectos personales propios de personas físicas, basada en la elaboración de perfiles de dichos datos o a raíz del tratamiento de categorías especiales de datos personales, datos biométricos o datos sobre condenas e infracciones penales o medidas de seguridad conexas. También es necesaria una evaluación de impacto relativa a la protección de datos para el control de zonas de acceso público a gran escala, en particular cuando se utilicen dispositivos optoelectrónicos o para cualquier otro tipo de operación cuando la autoridad de control competente considere que el tratamiento entrañe probablemente un alto riesgo para los derechos y libertades de los interesados, en particular porque impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato, o porque se efectúe sistemáticamente a gran escala. El tratamiento de datos personales no debe considerarse a gran escala si lo realiza, respecto de datos personales de pacientes o clientes, un solo médico, otro profesional de la salud o abogado. En estos casos, la evaluación de impacto de la protección de datos no debe ser obligatoria.

(92) Hay circunstancias en las que puede ser razonable y económico que una evaluación de impacto relativa a la protección de datos abarque más de un único proyecto, por ejemplo, en el caso de que las autoridades u organismos públicos prevean crear una aplicación o plataforma común de tratamiento, o si varios responsables proyecten introducir una aplicación o un entorno de tratamiento común en un sector o segmento empresarial o para una actividad horizontal de uso generalizado.

(93) Los Estados miembros, al adoptar el Derecho en el que se basa el desempeño de las funciones de la autoridad pública o el organismo público y que regula la operación o el conjunto de operaciones de tratamiento en cuestión, pueden considerar necesario llevar a cabo dicha evaluación con carácter previo a las actividades de tratamiento.

(94) Debe consultarse a la autoridad de control antes de iniciar las actividades de tratamiento si una evaluación de impacto relativa a la protección de datos muestra que, en ausencia de garantías, medidas de seguridad y mecanismos destinados a mitigar los riesgos, el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas físicas, y el responsable del tratamiento considera que el riesgo no puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación. Existe la probabilidad de que ese alto riesgo se deba a determinados tipos de tratamiento y al alcance y frecuencia de este, lo que también puede ocasionar daños y perjuicios o una injerencia en los derechos y libertades de la persona física. La autoridad de control debe responder a la solicitud de consulta dentro de un plazo determinado. Sin embargo, la ausencia de respuesta de la autoridad de control dentro de dicho plazo no debe obstar a cualquier intervención de dicha autoridad basada en las funciones y poderes que le atribuye el presente Reglamento, incluido el poder de prohibir operaciones de tratamiento. Como parte de dicho proceso de consulta, se puede presentar a la autoridad de control el resultado de una evaluación de impacto relativa a la protección de datos efectuada en relación con el tratamiento en cuestión, en particular las medidas previstas para mitigar los riesgos para los derechos y libertades de las personas físicas.

(95) El encargado del tratamiento debe asistir al responsable cuando sea necesario y a petición suya, a fin de asegurar que se cumplen las obligaciones que se derivan de la

realización de las evaluaciones de impacto relativas a la protección de datos y de la consulta previa a la autoridad de control.

(96) Deben llevarse también a cabo consultas con la autoridad de control en el curso de la tramitación de una medida legislativa o reglamentaria que establezca el tratamiento de datos personales, a fin de garantizar la conformidad del tratamiento previsto con el presente Reglamento y, en particular, de mitigar el riesgo que implique el tratamiento para el interesado.

(97) Al supervisar la observancia interna del presente Reglamento, el responsable o el encargado del tratamiento debe contar con la ayuda de una persona con conocimientos especializados del Derecho y la práctica en materia de protección de datos si el tratamiento lo realiza una autoridad pública, a excepción de los tribunales u otras autoridades judiciales independientes en el ejercicio de su función judicial, si el tratamiento lo realiza en el sector privado un responsable cuyas actividades principales consisten en operaciones de tratamiento a gran escala que requieren un seguimiento habitual y sistemático de los interesados, o si las actividades principales del responsable o del encargado consisten en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales. En el sector privado, las actividades principales de un responsable están relacionadas con sus actividades primarias y no están relacionadas con el tratamiento de datos personales como actividades auxiliares. El nivel de conocimientos especializados necesario se debe determinar, en particular, en función de las operaciones de tratamiento de datos que se lleven a cabo y de la protección exigida para los datos personales tratados por el responsable o el encargado. Tales delegados de protección de datos, sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente.

(98) Se debe incitar a las asociaciones u otros organismos que representen a categorías de responsables o encargados a que elaboren códigos de conducta, dentro de los límites fijados por el presente Reglamento, con el fin de facilitar su aplicación efectiva, teniendo en cuenta las características específicas del tratamiento llevado a cabo en determinados sectores y las necesidades específicas de las microempresas y las pequeñas y medianas empresas. Dichos códigos de conducta podrían en particular establecer las obligaciones de los responsables y encargados, teniendo en cuenta el riesgo probable para los derechos y libertades de las personas físicas que se derive del tratamiento.

(99) Al elaborar un código de conducta, o al modificar o ampliar dicho código, las asociaciones y otros organismos que representan a categorías de responsables o encargados deben consultar a las partes interesadas, incluidos los interesados cuando sea posible, y tener en cuenta las consideraciones transmitidas y las opiniones manifestadas en respuesta a dichas consultas.

(100) A fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes.

(101) Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales. El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión por el presente Reglamento, ni siquiera en las transferencias ulteriores de datos personales desde el tercer país u organización internacional a responsables y encargados en el mismo u otro tercer país u organización internacional. En todo caso, las transferencias a terceros países y organizaciones internacionales solo pueden llevarse a cabo de plena conformidad con el presente Reglamento. Una transferencia solo podría tener lugar si, a reserva de las demás disposiciones del presente Reglamento, el responsable o encargado cumple las disposiciones del presente Reglamento relativas a la transferencia de datos personales a terceros países u organizaciones internacionales.

(102) El presente Reglamento se entiende sin perjuicio de los acuerdos internacionales celebrados entre la Unión y terceros países que regulan la transferencia de datos personales, incluidas las oportunas garantías para los interesados. Los Estados miembros pueden celebrar acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales siempre que dichos acuerdos no afecten al presente Reglamento ni a ninguna otra disposición del Derecho de la Unión e incluyan un nivel adecuado de protección de los derechos fundamentales de los interesados.

(103) La Comisión puede decidir, con efectos para toda la Unión, que un tercer país, un territorio o un sector específico de un tercer país, o una organización internacional ofrece un nivel de protección de datos adecuado, aportando de esta forma en toda la Unión seguridad y uniformidad jurídicas en lo que se refiere al tercer país u organización internacional que se considera ofrece tal nivel de protección. En estos casos, se pueden realizar transferencias de datos personales a estos países sin que se requiera obtener otro tipo de autorización. La Comisión también puede decidir revocar esa decisión, previo aviso y completa declaración motivada al tercer país u organización internacional.

(104) En consonancia con los valores fundamentales en los que se basa la Unión, en particular la protección de los derechos humanos, la Comisión, en su evaluación del tercer país, o de un territorio o un sector específico de un tercer país, debe tener en cuenta de qué manera respeta un determinado tercer país respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos y su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal. En la adopción de una decisión de adecuación con respecto a un territorio o un sector específico de un tercer país se deben tener en cuenta criterios claros y objetivos, como las actividades concretas de tratamiento y el alcance de las normas jurídicas aplicables y la legislación vigente en el tercer país. El tercer país debe ofrecer garantías que aseguren un nivel adecuado de protección equivalente en lo esencial al ofrecido en la Unión, en particular cuando los datos personales son objeto de tratamiento en uno o varios sectores específicos. En particular, el tercer país debe garantizar que haya un control verdaderamente independiente de la protección de datos y establecer mecanismos de cooperación con las autoridades de protección de datos de los Estados miembros, así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas.

(105) Aparte de los compromisos internacionales adquiridos por el tercer país u organización internacional, la Comisión debe tener en cuenta las obligaciones resultantes de la participación del tercer país u organización internacional en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones. En particular, debe tenerse en cuenta la adhesión del país al Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo adicional. La Comisión debe consultar al Comité al evaluar el nivel de protección existente en terceros países u organizaciones internacionales.

(106) La Comisión debe supervisar la aplicación de las decisiones sobre el nivel de protección en un país tercero, un territorio o un sector específico de un país tercero, o una organización internacional, y la aplicación las decisiones adoptadas sobre la base del artículo 25, apartado 6, o el artículo 26, apartado 4, de la Directiva 95/46/CE. En sus decisiones de adecuación, la Comisión debe establecer un mecanismo para la revisión periódica de su aplicación. Dicha revisión periódica debe realizarse en colaboración con el tercer país u organización internacional de que se trate y tener en cuenta todos los cambios en la materia que se produzcan en dicho tercer país u organización internacional. A efectos de la supervisión y realización de las revisiones periódicas, la Comisión debe tomar en consideración las opiniones y conclusiones del Parlamento Europeo y del Consejo, así como de otros organismos y fuentes pertinentes. La Comisión debe evaluar, en un plazo razonable, la aplicación de dichas decisiones e informar de cualquier conclusión pertinente al Comité que, en el sentido del Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo [(12)], establece el presente Reglamento, y al Parlamento Europeo y el Consejo.

(107) La Comisión puede reconocer que un tercer país, un territorio o sector específico en un tercer país, o una organización internacional ya no garantiza un nivel de protección de

datos adecuado. En consecuencia, debe prohibirse la transferencia de datos personales a dicho tercer país u organización internacional, salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes, y a las excepciones aplicadas a situaciones específicas. En ese caso, debe establecerse la celebración de consultas entre la Comisión y esos terceros países u organizaciones internacionales. La Comisión debe informar en tiempo oportuno al tercer país u organización internacional de las razones y entablar consultas a fin de subsanar la situación.

(108) En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto. Las transferencias también pueden realizarlas autoridades o entidades públicas con entidades o autoridades públicas de terceros países o con organizaciones internacionales con competencias o funciones correspondientes, igualmente sobre la base de disposiciones incorporadas a acuerdos administrativos, como un memorando de entendimiento, que reconozcan derechos exigibles y efectivos a los interesados. Si las garantías figuran en acuerdos administrativos que no sean jurídicamente vinculantes se debe recabar la autorización de la autoridad de control competente.

(109) La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar a que los responsables o encargados incluyan las cláusulas tipo de protección de datos en un contrato más amplio, como un contrato entre dos encargados, o a que añadan otras cláusulas o garantías adicionales, siempre que no contradigan, directa o indirectamente, las cláusulas contractuales tipo adoptadas por la Comisión o por una autoridad de control, ni mermen los derechos o las libertades fundamentales de los interesados. Se debe alentar a los responsables y encargados del tratamiento a ofrecer garantías adicionales mediante compromisos contractuales que complementen las cláusulas tipo de protección de datos.

(110) Todo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta debe tener la posibilidad de invocar normas corporativas vinculantes autorizadas para sus transferencias internacionales de la Unión a organizaciones dentro del mismo grupo empresarial o unión de empresas dedicadas a una actividad económica conjunta, siempre que tales normas corporativas incorporen todos los principios esenciales y derechos aplicables con el fin de ofrecer garantías adecuadas para las transferencias o categorías de transferencias de datos de carácter personal.

(111) Se debe establecer la posibilidad de realizar transferencias en determinadas circunstancias, de mediar el consentimiento explícito del interesado, si la transferencia es ocasional y necesaria en relación con un contrato o una reclamación, independientemente de tratarse de un procedimiento judicial o un procedimiento administrativo o extrajudicial, incluidos los procedimientos ante organismos reguladores. También se debe establecer la posibilidad de realizar transferencias cuando así lo requieran razones importantes de interés público establecidas por el Derecho de la Unión o de los Estados miembros, o cuando la transferencia se haga a partir de un registro establecido por ley y se destine a consulta por el público o por personas que tengan un interés legítimo. En este último caso la transferencia no debe afectar a la totalidad de los datos personales o de las categorías de datos incluidos en el registro y, cuando el registro esté destinado a su consulta por personas que tengan un interés legítimo, la transferencia solo debe efectuarse a petición de dichas personas o, si

estas van a ser las destinatarias, teniendo plenamente en cuenta los intereses y los derechos fundamentales del interesado.

(112) Dichas excepciones deben aplicarse en particular a las transferencias de datos requeridas y necesarias por razones importantes de interés público, por ejemplo en caso de intercambios internacionales de datos entre autoridades en el ámbito de la competencia, administraciones fiscales o aduaneras, entre autoridades de supervisión financiera, entre servicios competentes en materia de seguridad social o de sanidad pública, por ejemplo en caso contactos destinados a localizar enfermedades contagiosas o para reducir y/o eliminar el dopaje en el deporte. La transferencia de datos personales también debe considerarse lícita en caso de que sea necesaria para proteger un interés esencial para los intereses vitales del interesado o de otra persona, incluida la integridad física o la vida, si el interesado no está en condiciones de dar su consentimiento. En ausencia de una decisión de adecuación, el Derecho de la Unión o de los Estados miembros puede limitar expresamente, por razones importantes de interés público, la transferencia de categorías específicas de datos a un tercer país o a una organización internacional. Los Estados miembros deben notificar esas disposiciones a la Comisión. Puede considerarse necesaria, por una razón importante de interés público o por ser de interés vital para el interesado, toda transferencia a una organización internacional humanitaria de datos personales de un interesado que no tenga capacidad física o jurídica para dar su consentimiento, con el fin de desempeñar un cometido basado en las Convenciones de Ginebra o de conformarse al Derecho internacional humanitario aplicable en caso de conflictos armados.

(113) Las transferencias que pueden calificarse de no repetitivas y sólo se refieren a un número limitado de interesados, también han de ser posibles en caso de servir a intereses legítimos imperiosos del responsable del tratamiento, si no prevalecen sobre ellos los intereses o los derechos y libertades del interesado y el responsable ha evaluado todas las circunstancias concurrentes en la transferencia de datos. El responsable debe prestar especial atención a la naturaleza de los datos personales, la finalidad y la duración de la operación o las operaciones de tratamiento propuestas, así como la situación en el país de origen, el tercer país y el país de destino final, y ofrecer, garantías apropiadas para proteger los derechos fundamentales y las libertades de las personas físicas con respecto al tratamiento de sus datos personales. Dichas transferencias sólo deben ser posibles en casos aislados, cuando ninguno de los otros motivos para la transferencia sean aplicables. Las legítimas expectativas de la sociedad en un aumento del conocimiento se deben tener en cuenta para fines de investigación científica o histórica o fines estadísticos. El responsable debe informar de la transferencia a la autoridad de control y al interesado.

(114) En cualquier caso, cuando la Comisión no haya tomado ninguna decisión sobre el nivel adecuado de la protección de datos en un tercer país, el responsable o el encargado del tratamiento deben arbitrar soluciones que garanticen a los interesados derechos exigibles y efectivos con respecto al tratamiento de sus datos en la Unión, una vez transferidos estos, de forma que sigan beneficiándose de derechos fundamentales y garantías.

(115) Algunos países terceros adoptan leyes, reglamentaciones y otros actos jurídicos con los que se pretende regular directamente las actividades de tratamiento de personas físicas y jurídicas bajo jurisdicción de los Estados miembros. Esto puede incluir sentencias de órganos jurisdiccionales o decisiones de autoridades administrativas de terceros países que obliguen a un responsable o un encargado del tratamiento a transferir o comunicar datos personales, y que no se basen en un acuerdo internacional, como un tratado de asistencia judicial mutua, en vigor entre el tercer país requirente y la Unión o un Estado miembro. La aplicación extraterritorial de dichas leyes, reglamentaciones y otros actos jurídicos puede ser contraria al Derecho internacional e impedir la protección de las personas físicas garantizada en la Unión en virtud del presente Reglamento. Las transferencias solo deben autorizarse cuando se cumplan las condiciones del presente Reglamento relativas a las transferencias a terceros países. Tal puede ser el caso, entre otros, cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento.

(116) Cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer

los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información. Al mismo tiempo, es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras. Sus esfuerzos por colaborar en el contexto transfronterizo también pueden verse obstaculizados por poderes preventivos o correctivos insuficientes, regímenes jurídicos incoherentes y obstáculos prácticos, como la escasez de recursos. Por consiguiente, es necesario fomentar una cooperación más estrecha entre las autoridades de control encargadas de la protección de datos para ayudarlas a intercambiar información y a llevar a cabo investigaciones con sus homólogos internacionales. A fin de desarrollar mecanismos de cooperación internacional que faciliten y proporcionen asistencia internacional mutua en la ejecución de legislación en materia de protección de datos personales, la Comisión y las autoridades de control deben intercambiar información y cooperar en actividades relativas al ejercicio de sus competencias con las autoridades competentes de terceros países, sobre la base de la reciprocidad y de conformidad con el presente Reglamento.

(117) El establecimiento en los Estados miembros de autoridades de control capacitadas para desempeñar sus funciones y ejercer sus competencias con plena independencia constituye un elemento esencial de la protección de las personas físicas con respecto al tratamiento de datos de carácter personal. Los Estados miembros deben tener la posibilidad de establecer más de una autoridad de control, a fin de reflejar su estructura constitucional, organizativa y administrativa.

(118) La independencia de las autoridades de control no debe significar que dichas autoridades puedan quedar exentas de mecanismos de control o supervisión en relación con sus gastos financieros, o de control judicial.

(119) Si un Estado miembro establece varias autoridades de control, debe disponer por ley mecanismos que garanticen la participación efectiva de dichas autoridades de control en el mecanismo de coherencia. Tal Estado miembro debe, en particular, designar a la autoridad de control que actuará como punto de contacto único de cara a la participación efectiva de dichas autoridades en el citado mecanismo, garantizando así una cooperación rápida y fluida con otras autoridades de control, el Comité y la Comisión.

(120) Todas las autoridades de control deben estar dotadas de los recursos financieros y humanos, los locales y las infraestructuras que sean necesarios para la realización eficaz de sus funciones, en particular las relacionadas con la asistencia recíproca y la cooperación con otras autoridades de control de la Unión. Cada autoridad de control debe disponer de un presupuesto anual público propio, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

(121) Las condiciones generales aplicables al miembro o los miembros de la autoridad de control deben establecerse por ley en cada Estado miembro y disponer, en particular, que dichos miembros han de ser nombrados, por un procedimiento transparente, por el Parlamento, el Gobierno o el jefe de Estado del Estado miembro, a propuesta del Gobierno, de un miembro del Gobierno o del Parlamento o una de sus cámaras, o por un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros. A fin de garantizar la independencia de la autoridad de control, sus miembros deben actuar con integridad, abstenerse de cualquier acción que sea incompatible con sus funciones y no participar, mientras dure su mandato, en ninguna actividad profesional incompatible, sea o no remunerada. La autoridad de control debe tener su propio personal, seleccionado por esta o por un organismo independiente establecido por el Derecho de los Estados miembros, que esté subordinado exclusivamente al miembro o los miembros de la autoridad de control.

(122) Cada autoridad de control debe ser competente, en el territorio de su Estado miembro, para ejercer los poderes y desempeñar las funciones que se le confieran de conformidad con el presente Reglamento. Lo anterior debe abarcar, en particular, el tratamiento en el contexto de las actividades de un establecimiento del responsable o del encargado en el territorio de su Estado miembro, el tratamiento de datos personales realizado por autoridades públicas o por organismos privados que actúen en interés público, el tratamiento que afecte a interesados en su territorio, o el tratamiento realizado por un responsable o un encargado que no esté establecido en la Unión cuando sus destinatarios sean interesados residentes en su territorio. Debe incluirse el examen de reclamaciones

presentadas por un interesado, la realización de investigaciones sobre la aplicación del presente Reglamento y el fomento de la sensibilización del público acerca de los riesgos, las normas, las garantías y los derechos en relación con el tratamiento de datos personales.

(123) A fin de proteger a las personas físicas con respecto al tratamiento de sus datos personales y de facilitar la libre circulación de los datos personales en el mercado interior, las autoridades de control deben supervisar la aplicación de las disposiciones adoptadas de conformidad con el presente Reglamento y contribuir a su aplicación coherente en toda la Unión. A tal efecto, las autoridades de control deben cooperar entre ellas y con la Comisión, sin necesidad de acuerdo alguno entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación.

(124) Si el tratamiento de datos personales se realiza en el contexto de las actividades de un establecimiento de un responsable o un encargado en la Unión y el responsable o el encargado está establecido en más de un Estado miembro, o si el tratamiento en el contexto de las actividades de un único establecimiento de un responsable o un encargado en la Unión afecta o es probable que afecte sustancialmente a interesados en más de un Estado miembro, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado debe actuar como autoridad principal. Dicha autoridad debe cooperar con las demás autoridades interesadas, ya sea porque el responsable o el encargado tenga un establecimiento en el territorio de su Estado miembro, porque afecte sustancialmente a interesados que residen en su territorio, o porque se haya presentado una reclamación ante ellas. Asimismo, cuando un interesado que no resida en ese Estado miembro haya presentado una reclamación, la autoridad de control ante la que se haya presentado esta también debe ser autoridad de control interesada. En el marco de sus funciones de formulación de directrices sobre cualquier cuestión relacionada con la aplicación del presente Reglamento, el Comité debe estar facultado para formular directrices, en particular sobre los criterios que han de tenerse en cuenta para determinar si el tratamiento en cuestión afecta sustancialmente a interesados de más de un Estado miembro y sobre lo que constituya una objeción pertinente y motivada.

(125) La autoridad principal debe ser competente para adoptar decisiones vinculantes relativas a las medidas de aplicación de los poderes conferidos con arreglo al presente Reglamento. En su calidad de autoridad principal, la autoridad de control debe implicar estrechamente y coordinar a las autoridades de control interesadas en el proceso de toma de decisiones. En los casos en los que la decisión consista en rechazar total o parcialmente la reclamación del interesado, esa decisión debe ser adoptada por la autoridad de control ante la que se haya presentado la reclamación.

(126) La decisión debe ser acordada conjuntamente por la autoridad de control principal y las autoridades de control interesadas y debe dirigirse al establecimiento principal o único del responsable o del encargado del tratamiento y ser vinculante para ambos. El responsable o el encargado deben tomar las medidas necesarias para garantizar el cumplimiento del presente Reglamento y la aplicación de la decisión notificada por la autoridad de control principal al establecimiento principal del responsable o del encargado en lo que se refiere a las actividades de tratamiento en la Unión.

(127) Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado. Al decidir si trata el asunto, la autoridad de control principal debe considerar si existe un establecimiento del responsable o del encargado en el Estado miembro de la autoridad de control que le haya informado, con el fin de garantizar la ejecución efectiva de la decisión respecto del responsable o encargado del tratamiento. Si la

autoridad de control principal decide tratar el asunto, se debe ofrecer a la autoridad de control informante la posibilidad de presentar un proyecto de decisión, que la autoridad de control principal ha de tener en cuenta en la mayor medida posible al preparar su proyecto de decisión al amparo del mecanismo de ventanilla única.

(128) Las normas sobre la autoridad de control principal y el mecanismo de ventanilla única no deben aplicarse cuando el tratamiento sea realizado por autoridades públicas u organismos privados en interés público. En tales casos, la única autoridad de control competente para ejercer los poderes conferidos con arreglo al presente Reglamento debe ser la autoridad de control del Estado miembro en el que estén establecidos la autoridad pública o el organismo privado.

(129) Para garantizar la supervisión y ejecución coherentes del presente Reglamento en toda la Unión, las autoridades de control deben tener en todos los Estados miembros las mismas funciones y poderes efectivos, incluidos poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos, especialmente en casos de reclamaciones de personas físicas, y sin perjuicio de las competencias de las autoridades encargadas de la persecución de los delitos con arreglo al Derecho de los Estados miembros para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y ejercitar acciones judiciales. Dichos poderes deben incluir también el poder de imponer una limitación temporal o definitiva al tratamiento, incluida su prohibición. Los Estados miembros pueden especificar otras funciones relacionadas con la protección de datos personales con arreglo al presente Reglamento. Los poderes de las autoridades de control deben ejercerse de conformidad con garantías procesales adecuadas establecidas en el Derecho de la Unión y los Estados miembros, de forma imparcial, equitativa y en un plazo razonable. En particular, toda medida debe ser adecuada, necesaria y proporcionada con vistas a garantizar el cumplimiento del presente Reglamento, teniendo en cuenta las circunstancias de cada caso concreto, respetar el derecho de todas las personas a ser oídas antes de que se adopte cualquier medida que las afecte negativamente y evitar costes superfluos y molestias excesivas para las personas afectadas. Los poderes de investigación en lo que se refiere al acceso a instalaciones deben ejercerse de conformidad con los requisitos específicos del Derecho procesal de los Estados miembros, como el de la autorización judicial previa. Toda medida jurídicamente vinculante de la autoridad de control debe constar por escrito, ser clara e inequívoca, indicar la autoridad de control que dictó la medida y la fecha en que se dictó, llevar la firma del director o de un miembro de la autoridad de control autorizado por este, especificar los motivos de la medida y mencionar el derecho a la tutela judicial efectiva. Esto no debe obstar a que se impongan requisitos adicionales con arreglo al Derecho procesal de los Estados miembros. La adopción de una decisión jurídicamente vinculante implica que puede ser objeto de control judicial en el Estado miembro de la autoridad de control que adoptó la decisión.

(130) Cuando la autoridad de control ante la cual se haya presentado la reclamación no sea la autoridad de control principal, esta última debe cooperar estrechamente con la primera con arreglo a las disposiciones sobre cooperación y coherencia establecidas en el presente Reglamento. En tales casos, la autoridad de control principal, al tomar medidas concebidas para producir efectos jurídicos, incluida la imposición de multas administrativas, debe tener en cuenta en la mayor medida posible la opinión de la autoridad de control ante la cual se haya presentado la reclamación y la cual debe seguir siendo competente para realizar cualquier investigación en el territorio de su propio Estado miembro en enlace con la autoridad de control competente.

(131) En casos en los que otra autoridad de control deba actuar como autoridad de control principal para las actividades de tratamiento del responsable o del encargado pero el objeto concreto de una reclamación o la posible infracción afecta únicamente a las actividades de tratamiento del responsable o del encargado en el Estado miembro en el que se haya presentado la reclamación o detectado la posible infracción y el asunto no afecta sustancialmente ni es probable que afecte sustancialmente a interesados de otros Estados miembros, la autoridad de control que reciba una reclamación o que detecte situaciones que conlleven posibles infracciones del presente Reglamento o reciba de otra manera información sobre estas debe tratar de llegar a un arreglo amistoso con el responsable del tratamiento y, si no prospera, ejercer todos sus poderes. En lo anterior se debe incluir el

tratamiento específico realizado en el territorio del Estado miembro de la autoridad de control o con respecto a interesados en el territorio de dicho Estado miembro; el tratamiento efectuado en el contexto de una oferta de bienes o servicios destinada específicamente a interesados en el territorio del Estado miembro de la autoridad de control; o el tratamiento que deba evaluarse teniendo en cuenta las obligaciones legales pertinentes en virtud del Derecho de los Estados miembros.

(132) Entre las actividades de sensibilización del público por parte de las autoridades de control deben incluirse medidas específicas dirigidas a los responsables y los encargados del tratamiento, incluidas las microempresas y las pequeñas y medianas empresas, así como las personas físicas, en particular en el contexto educativo.

(133) Las autoridades de control se deben ayudar una a otra en el desempeño de sus funciones y prestar asistencia mutua, con el fin de garantizar la aplicación y ejecución coherentes del presente Reglamento en el mercado interior. Una autoridad de control que solicite asistencia mutua puede adoptar una medida provisional si no recibe respuesta a su solicitud de asistencia en el plazo de un mes a partir de su recepción por la otra autoridad de control.

(134) Cada autoridad de control debe participar, cuando proceda, en operaciones conjuntas con otras autoridades de control. La autoridad de control a la que se solicite ayuda debe tener la obligación de responder a la solicitud en un plazo de tiempo determinado.

(135) A fin de garantizar la aplicación coherente del presente Reglamento en toda la Unión, debe establecerse un mecanismo de coherencia para la cooperación entre las autoridades de control. Este mecanismo debe aplicarse en particular cuando una autoridad de control prevea adoptar una medida dirigida a producir efectos jurídicos en lo que se refiere a operaciones de tratamiento que afecten sustancialmente a un número significativo de interesados en varios Estados miembros. También debe aplicarse cuando cualquier autoridad de control interesada o la Comisión soliciten que dicho asunto se trate al amparo del mecanismo de coherencia. Dicho mecanismo debe entenderse sin perjuicio de cualesquiera medidas que la Comisión pueda adoptar en el ejercicio de sus poderes con arreglo a los Tratados.

(136) En aplicación del mecanismo de coherencia, el Comité debe, en un plazo determinado, emitir un dictamen, si así lo decide una mayoría de sus miembros o si así lo solicita cualquier autoridad de control interesada o la Comisión. El Comité también debe estar facultado para adoptar decisiones jurídicamente vinculantes en caso de diferencias entre autoridades de control. A tal efecto debe dictar, en principio por mayoría de dos tercios de sus miembros, decisiones jurídicamente vinculantes en casos claramente especificados en los que exista conflicto de opiniones entre las autoridades de control, en particular en el mecanismo de cooperación entre la autoridad de control principal y las autoridades de control interesadas sobre el fondo del asunto, especialmente en caso de infracción del presente Reglamento.

(137) La necesidad urgente de actuar puede obedecer a la necesidad de proteger los derechos y libertades de los interesados, en particular cuando exista el riesgo de que pueda verse considerablemente obstaculizado el reconocimiento de alguno de sus derechos. Por lo tanto, una autoridad de control debe poder adoptar en su territorio medidas provisionales, debidamente justificadas, con un plazo de validez determinado no superior a tres meses.

(138) La aplicación de tal mecanismo debe ser una condición para la licitud de una medida de una autoridad de control destinada a producir efectos jurídicos, en aquellos casos en los que su aplicación sea obligatoria. En otros casos de relevancia transfronteriza, la autoridad de control principal y las autoridades de control interesadas deben aplicar entre sí el mecanismo de cooperación, y las autoridades de control interesadas pueden prestarse asistencia mutua y realizar entre sí operaciones conjuntas, sobre una base bilateral o multilateral, sin tener que aplicarlo.

(139) A fin de fomentar la aplicación coherente del presente Reglamento, el Comité debe constituirse como organismo independiente de la Unión. Para cumplir sus objetivos, el Comité debe tener personalidad jurídica. Su presidente debe ostentar su representación. El Comité debe sustituir al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales creado por la Directiva 95/46/CE. Debe estar compuesto por el director de una autoridad de control de cada Estado miembro y el Supervisor Europeo de

Protección de Datos, o por sus respectivos representantes. La Comisión debe participar en las actividades del Comité sin derecho a voto y se deben reconocer derechos de voto específicos al Supervisor Europeo de Protección de Datos. El Comité debe contribuir a la aplicación coherente del presente Reglamento en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión. El Comité debe actuar con independencia en el cumplimiento de sus funciones.

(140) El Comité debe contar con una secretaría, a cargo el Supervisor Europeo de Protección de Datos. El personal del Supervisor Europeo de Protección de Datos que participe en la realización de las funciones conferidas al Comité por el presente Reglamento debe desempeñar sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité y responder ante él.

(141) Todo interesado debe tener derecho a presentar una reclamación ante una autoridad de control única, en particular en el Estado miembro de su residencia habitual, y derecho a la tutela judicial efectiva de conformidad con el artículo 47 de la Carta si considera que se vulneran sus derechos con arreglo al presente Reglamento o en caso de que la autoridad de control no responda a una reclamación, rechace o desestime total o parcialmente una reclamación o no actúe cuando sea necesario para proteger los derechos del interesado. La investigación a raíz de una reclamación debe llevarse a cabo, bajo control judicial, si procede en el caso concreto. La autoridad de control debe informar al interesado de la evolución y el resultado de la reclamación en un plazo razonable. Si el asunto requiere una mayor investigación o coordinación con otra autoridad de control, se debe facilitar información intermedia al interesado. Para facilitar la presentación de reclamaciones, cada autoridad de control debe adoptar medidas como el suministro de un formulario de reclamaciones, que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

(142) El interesado que considere vulnerados los derechos reconocidos por el presente Reglamento debe tener derecho a conferir mandato a una entidad, organización o asociación sin ánimo de lucro que esté constituida con arreglo al Derecho de un Estado miembro, tenga objetivos estatutarios que sean de interés público y actúe en el ámbito de la protección de los datos personales, para que presente en su nombre una reclamación ante la autoridad de control, ejerza el derecho a la tutela judicial en nombre de los interesados o, si así lo establece el Derecho del Estado miembro, ejerza el derecho a recibir una indemnización en nombre de estos. Un Estado miembro puede reconocer a tal entidad, organización o asociación el derecho a presentar en él una reclamación con independencia del mandato de un interesado y el derecho a la tutela judicial efectiva, cuando existan motivos para creer que se han vulnerado los derechos de un interesado como consecuencia de un tratamiento de datos personales que sea contrario al presente Reglamento. Esa entidad, organización o asociación no puede estar autorizada a reclamar una indemnización en nombre de un interesado al margen del mandato de este último.

(143) Toda persona física o jurídica tiene derecho a interponer ante el Tribunal de Justicia recurso de anulación de decisiones del Comité, en las condiciones establecidas en el artículo 263 del TFUE. Como destinatarias de dichas decisiones, las autoridades de control interesadas que quieran impugnarlas tienen que interponer recurso en el plazo de dos meses a partir del momento en que les fueron notificadas, de conformidad con el artículo 263 del TFUE. En caso de que las decisiones del Comité afecten directa e individualmente a un responsable, un encargado o al reclamante, estos pueden interponer recurso de anulación de dichas decisiones en el plazo de dos meses a partir de su publicación en el sitio web del Comité, de conformidad con el artículo 263 del TFUE. Sin perjuicio de lo dispuesto en el artículo 263 del TFUE, toda persona física o jurídica debe tener derecho a la tutela judicial efectiva ante el tribunal nacional competente contra las decisiones de una autoridad de control que produzcan efectos jurídicos que le afecten. Tales decisiones se refieren en particular al ejercicio de los poderes de investigación, corrección y autorización por parte de la autoridad de control o a la desestimación o rechazo de reclamaciones. No obstante, el derecho a la tutela judicial efectiva no incluye medidas adoptadas por las autoridades de control que no sean jurídicamente vinculantes, como los dictámenes publicados o el

asesoramiento facilitado por ellas. Las acciones contra una autoridad de control deben ejercitarse ante los tribunales del Estado miembro en el que esté establecida y tramitarse con arreglo al Derecho procesal de dicho Estado miembro. Dichos tribunales deben tener plena jurisdicción, incluida la competencia para examinar todos los elementos de hecho y de Derecho relativos a la causa de la que conozcan.

Si una autoridad de control rechaza o desestima una reclamación, el reclamante puede ejercitar una acción ante los tribunales del mismo Estado miembro. En el contexto de las acciones judiciales relacionadas con la aplicación del presente Reglamento, los tribunales nacionales que estimen necesaria una decisión al respecto para poder emitir su fallo pueden, o en el caso establecido en el artículo 267 del TFUE, deben solicitar al Tribunal de Justicia que se pronuncie con carácter prejudicial sobre la interpretación del Derecho de la Unión, incluido el presente Reglamento. Además, si una decisión de una autoridad de control por la que se ejecuta una decisión del Comité se impugna ante un tribunal nacional y se cuestiona la validez de la decisión del Comité, dicho tribunal nacional no es competente para declarar inválida la decisión del Comité, sino que, si la considera inválida, tiene que remitir la cuestión de la validez al Tribunal de Justicia de conformidad con el artículo 267 del TFUE, según la interpretación de este. No obstante, un tribunal nacional puede no remitir la cuestión de la validez de la decisión del Comité a instancia de una persona física o jurídica que, habiendo tenido la oportunidad de interponer recurso de anulación de dicha decisión, en particular si dicha decisión la afectaba directa e individualmente, no lo hizo en el plazo establecido en el artículo 263 del TFUE.

(144) Si un tribunal ante el cual se ejercitaron acciones contra una decisión de una autoridad de control tiene motivos para creer que se ejercitaron acciones ante un tribunal competente de otro Estado miembro relativas al mismo tratamiento, como tener el mismo asunto con respecto a un tratamiento por el mismo responsable o encargado, o la misma causa de la acción, debe ponerse en contacto con ese tribunal para confirmar la existencia de tales acciones conexas. Si dichas acciones conexas están pendientes ante un tribunal de otro Estado miembro, cualquier otro tribunal distinto de aquel ante el cual se ejercitó la acción en primer lugar puede suspender el procedimiento o, a instancia de una de las partes, inhibirse a favor del tribunal ante el cual se ejercitó la acción en primer lugar si este último es competente para su conocimiento y su acumulación es conforme a Derecho. Se consideran conexas las acciones vinculadas entre sí por una relación tan estrecha que procede tramitarlas y resolverlas conjuntamente a fin de evitar resoluciones que podrían ser incompatibles si se sustanciaran como causas separadas.

(145) Por lo que respecta a las acciones contra los responsables o encargados del tratamiento, el reclamante debe tener la opción de ejercitarlas ante los tribunales de los Estados miembros en los que el responsable o el encargado tenga un establecimiento o resida el interesado, a menos que el responsable sea una autoridad pública de un Estado miembro que actúe en el ejercicio de poderes públicos.

(146) El responsable o el encargado del tratamiento debe indemnizar cualesquiera daños y perjuicios que pueda sufrir una persona como consecuencia de un tratamiento en infracción del presente Reglamento. El responsable o el encargado deben quedar exentos de responsabilidad si se demuestra que en modo alguno son responsables de los daños y perjuicios. El concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento. Lo anterior se entiende sin perjuicio de cualquier reclamación por daños y perjuicios derivada de la vulneración de otras normas del Derecho de la Unión o de los Estados miembros. Un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento. Los interesados deben recibir una indemnización total y efectiva por los daños y perjuicios sufridos. Si los responsables o encargados participan en el mismo tratamiento, cada responsable o encargado debe ser considerado responsable de la totalidad de los daños y perjuicios. No obstante, si se acumulan en la misma causa de conformidad con el Derecho de los Estados miembros, la indemnización puede prorratearse en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre

que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios. Todo responsable o encargado que haya abonado la totalidad de la indemnización puede interponer recurso posteriormente contra otros responsables o encargados que hayan participado en el mismo tratamiento.

(147) En los casos en que el presente Reglamento contiene normas específicas sobre competencia judicial, en particular por lo que respecta a las acciones que tratan de obtener satisfacción por la vía judicial, incluida la indemnización, contra un responsable o encargado del tratamiento, las normas generales de competencia judicial como las establecidas en el Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo [13] deben entenderse sin perjuicio de la aplicación de dichas normas específicas.

(148) A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento. Debe no obstante prestarse especial atención a la naturaleza, gravedad y duración de la infracción, a su carácter intencional, a las medidas tomadas para paliar los daños y perjuicios sufridos, al grado de responsabilidad o a cualquier infracción anterior pertinente, a la forma en que la autoridad de control haya tenido conocimiento de la infracción, al cumplimiento de medidas ordenadas contra el responsable o encargado, a la adhesión a códigos de conducta y a cualquier otra circunstancia agravante o atenuante. La imposición de sanciones, incluidas las multas administrativas, debe estar sujeta a garantías procesales suficientes conforme a los principios generales del Derecho de la Unión y de la Carta, entre ellas el derecho a la tutela judicial efectiva y a un proceso con todas las garantías.

(149) Los Estados miembros deben tener la posibilidad de establecer normas en materia de sanciones penales por infracciones del presente Reglamento, incluidas las infracciones de normas nacionales adoptadas con arreglo a él y dentro de sus límites. Dichas sanciones penales pueden asimismo autorizar la privación de los beneficios obtenidos en infracción del presente Reglamento. No obstante, la imposición de sanciones penales por infracciones de dichas normas nacionales y de sanciones administrativas no debe entrañar la vulneración del principio ne bis in idem, según la interpretación del Tribunal de Justicia.

(150) A fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas. El presente Reglamento debe indicar las infracciones así como el límite máximo y los criterios para fijar las correspondientes multas administrativas, que la autoridad de control competente debe determinar en cada caso individual teniendo en cuenta todas las circunstancias concurrentes en él, atendiendo en particular a la naturaleza, gravedad y duración de la infracción y sus consecuencias y a las medidas tomadas para garantizar el cumplimiento de las obligaciones impuestas por el presente Reglamento e impedir o mitigar las consecuencias de la infracción. Si las multas administrativas se imponen a una empresa, por tal debe entenderse una empresa con arreglo a los artículos 101 y 102 del TFUE. Si las multas administrativas se imponen a personas que no son una empresa, la autoridad de control debe tener en cuenta al valorar la cuantía apropiada de la multa el nivel general de ingresos prevaleciente en el Estado miembro así como la situación económica de la persona. El mecanismo de coherencia también puede emplearse para fomentar una aplicación coherente de las multas administrativas. Debe corresponder a los Estados miembros determinar si y en qué medida se debe imponer multas administrativas a las autoridades públicas. La imposición de una multa administrativa o de una advertencia no afecta al ejercicio de otras competencias de las autoridades de control ni a la aplicación de otras sanciones al amparo del presente Reglamento.

(151) Los ordenamientos jurídicos de Dinamarca y Estonia no permiten las multas administrativas según lo dispuesto en el presente Reglamento. Las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por la autoridad de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto

equivalente a las multas administrativas impuestas por las autoridades de control. Por lo tanto los tribunales nacionales competentes deben tener en cuenta la recomendación de la autoridad de control que incoe la multa. En todo caso, las multas impuestas deben ser efectivas, proporcionadas y disuasorias.

(152) En los casos en que el presente Reglamento no armoniza las sanciones administrativas, o en otros casos en que se requiera, por ejemplo en casos de infracciones graves del presente Reglamento, los Estados miembros deben aplicar un sistema que establezca sanciones efectivas, proporcionadas y disuasorias. La naturaleza de dichas sanciones, ya sea penal o administrativa, debe ser determinada por el Derecho de los Estados miembros.

(153) El Derecho de los Estados miembros debe conciliar las normas que rigen la libertad de expresión e información, incluida la expresión periodística, académica, artística o literaria, con el derecho a la protección de los datos personales con arreglo al presente Reglamento. El tratamiento de datos personales con fines exclusivamente periodísticos o con fines de expresión académica, artística o literaria debe estar sujeto a excepciones o exenciones de determinadas disposiciones del presente Reglamento si así se requiere para conciliar el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información consagrado en el artículo 11 de la Carta. Esto debe aplicarse en particular al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas. Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos. Si dichas exenciones o excepciones difieren de un Estado miembro a otro debe regir el Derecho del Estado miembro que sea aplicable al responsable del tratamiento. A fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio.

(154) El presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento. La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos. La Directiva 2003/98/CE del Parlamento Europeo y del Consejo [(14)] no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales.

(155) El Derecho de los Estados miembros o los convenios colectivos, incluidos los «convenios de empresa», pueden establecer normas específicas relativas al tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular en relación con las condiciones en las que los datos personales en el contexto laboral pueden ser objeto de tratamiento sobre la base del consentimiento del trabajador, los fines de la contratación, la

ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por convenio colectivo, la gestión, planificación y organización del trabajo, la igualdad y seguridad en el lugar de trabajo, la salud y seguridad en el trabajo, así como a los fines del ejercicio y disfrute, sea individual o colectivo, de derechos y prestaciones relacionados con el empleo y a efectos de la rescisión de la relación laboral.

(156) El tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos debe estar supeditado a unas garantías adecuadas para los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, el principio de minimización de los datos. El tratamiento ulterior de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos ha de efectuarse cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante un tratamiento de datos que no permita identificar a los interesados, o que ya no lo permita, siempre que existan las garantías adecuadas (como, por ejemplo, la seudonimización de datos). Los Estados miembros deben establecer garantías adecuadas para el tratamiento de datos personales con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. Debe autorizarse que los Estados miembros establezcan, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición, cuando se traten datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos. Las condiciones y garantías en cuestión pueden conllevar procedimientos específicos para que los interesados ejerzan dichos derechos si resulta adecuado a la luz de los fines perseguidos por el tratamiento específico, junto con las medidas técnicas y organizativas destinadas a minimizar el tratamiento de datos personales atendiendo a los principios de proporcionalidad y necesidad. El tratamiento de datos personales con fines científicos también debe observar otras normas pertinentes, como las relativas a los ensayos clínicos.

(157) Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros.

(158) El presente Reglamento también debe aplicarse al tratamiento de datos personales realizado con fines de archivo, teniendo presente que no debe se de aplicación a personas fallecidas. Las autoridades públicas o los organismos públicos o privados que llevan registros de interés público deben ser servicios que están obligados, con arreglo al Derecho de la Unión o de los Estados miembros, a adquirir, mantener, evaluar, organizar, describir, comunicar, promover y difundir registros de valor perdurable para el interés público general y facilitar acceso a ellos. Los Estados miembros también debe estar autorizados a establecer el tratamiento ulterior de datos personales con fines de archivo, por ejemplo a fin de ofrecer información específica relacionada con el comportamiento político bajo antiguos regímenes de Estados totalitarios, el genocidio, los crímenes contra la humanidad, en particular el Holocausto, o los crímenes de guerra.

(159) El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de

manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. Para cumplir las especificidades del tratamiento de datos personales con fines de investigación científica deben aplicarse condiciones específicas, en particular en lo que se refiere a la publicación o la comunicación de otro modo de datos personales en el contexto de fines de investigación científica. Si el resultado de la investigación científica, en particular en el ámbito de la salud, justifica otras medidas en beneficio del interesado, las normas generales del presente Reglamento deben aplicarse teniendo en cuenta tales medidas.

(160) El presente Reglamento debe aplicarse asimismo al tratamiento datos personales que se realiza con fines de investigación histórica. Esto incluye asimismo la investigación histórica y la investigación para fines genealógicos, teniendo en cuenta que el presente Reglamento no es de aplicación a personas fallecidas.

(161) Al objeto de otorgar el consentimiento para la participación en actividades de investigación científica en ensayos clínicos, deben aplicarse las disposiciones pertinentes del Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo [(15)].

(162) El presente Reglamento debe aplicarse al tratamiento de datos personales con fines estadísticos. El contenido estadístico, el control de accesos, las especificaciones para el tratamiento de datos personales con fines estadísticos y las medidas adecuadas para salvaguardar los derechos y las libertades de los interesados y garantizar la confidencialidad estadística deben ser establecidos, dentro de los límites del presente Reglamento, por el Derecho de la Unión o de los Estados miembros. Por fines estadísticos se entiende cualquier operación de recogida y tratamiento de datos personales necesarios para encuestas estadísticas o para la producción de resultados estadísticos. Estos resultados estadísticos pueden además utilizarse con diferentes fines, incluidos fines de investigación científica. El fin estadístico implica que el resultado del tratamiento con fines estadísticos no sean datos personales, sino datos agregados, y que este resultado o los datos personales no se utilicen para respaldar medidas o decisiones relativas a personas físicas concretas.

(163) Debe protegerse la información confidencial que las autoridades estadísticas de la Unión y nacionales recojan para la elaboración de las estadísticas oficiales europeas y nacionales. Las estadísticas europeas deben desarrollarse, elaborarse y difundirse con arreglo a los principios estadísticos fijados en el artículo 338, apartado 2, del TFUE, mientras que las estadísticas nacionales deben cumplir asimismo el Derecho de los Estados miembros. El Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo [(16)] facilita especificaciones adicionales sobre la confidencialidad estadística aplicada a las estadísticas europeas.

(164) Por lo que respecta a los poderes de las autoridades de control para obtener del responsable o del encargado del tratamiento acceso a los datos personales y a sus locales, los Estados miembros pueden adoptar por ley, dentro de los límites fijados por el presente Reglamento, normas específicas con vistas a salvaguardar el deber de secreto profesional u obligaciones equivalentes, en la medida necesaria para conciliar el derecho a la protección de los datos personales con el deber de secreto profesional. Lo anterior se entiende sin perjuicio de las obligaciones existentes para los Estados miembros de adoptar normas sobre el secreto profesional cuando así lo exija el Derecho de la Unión.

(165) El presente Reglamento respeta y no prejuzga el estatuto reconocido en los Estados miembros, en virtud del Derecho constitucional, a las iglesias y las asociaciones o comunidades religiosas, tal como se reconoce en el artículo 17 del TFUE.

(166) A fin de cumplir los objetivos del presente Reglamento, a saber, proteger los derechos y las libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, y garantizar la libre circulación de los datos personales en la Unión, debe delegarse en la Comisión el poder de adoptar actos de conformidad con el artículo 290 del TFUE. En particular, deben adoptarse actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar

dichos iconos. Reviste especial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y redactar los actos delegados, la Comisión debe garantizar la transmisión simultánea, oportuna y apropiada de los documentos pertinentes al Parlamento Europeo y al Consejo.

(167) A fin de garantizar condiciones uniformes de ejecución del presente Reglamento, deben conferirse a la Comisión competencias de ejecución cuando así lo establezca el presente Reglamento. Dichas competencias deben ejercerse de conformidad con el Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo. En este contexto, la Comisión debe considerar la adopción de medidas específicas para las microempresas y las pequeñas y medianas empresas.

(168) El procedimiento de examen debe seguirse para la adopción de actos de ejecución sobre cláusulas contractuales tipo entre responsables y encargados del tratamiento y entre responsables del tratamiento; códigos de conducta; normas técnicas y mecanismos de certificación; el nivel adecuado de protección ofrecido por un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional; cláusulas tipo de protección; formatos y procedimientos para el intercambio de información entre responsables, encargados y autoridades de control respecto de normas corporativas vinculantes; asistencia mutua; y modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre las autoridades de control y el Comité.

(169) La Comisión debe adoptar actos de ejecución inmediatamente aplicables cuando las pruebas disponibles muestren que un tercer país, un territorio o un sector específico en ese tercer país, o una organización internacional no garantizan un nivel de protección adecuado y así lo requieran razones imperiosas de urgencia.

(170) Dado que el objetivo del presente Reglamento, a saber, garantizar un nivel equivalente de protección de las personas físicas y la libre circulación de datos personales en la Unión Europea, no puede ser alcanzado de manera suficiente por los Estados miembros, sino que, debido a las dimensiones o los efectos de la acción, puede lograrse mejor a escala de la Unión, esta puede adoptar medidas, de acuerdo con el principio de subsidiariedad establecido en el artículo 5 del Tratado de la Unión Europea (TUE). De conformidad con el principio de proporcionalidad establecido en el mismo artículo, el presente Reglamento no excede de lo necesario para alcanzar dicho objetivo.

(171) La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas.

(172) De conformidad con el artículo 28, apartado 2, del Reglamento (CE) n.º 45/2001, se consultó al Supervisor Europeo de Protección de Datos, y éste emitió su dictamen el 7 de marzo de 2012 [(17)].

(173) El presente Reglamento debe aplicarse a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales en relación con el tratamiento de datos personales que no están sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE del Parlamento Europeo y del Consejo [(18)], incluidas las obligaciones del responsable del tratamiento y los derechos de las personas físicas. Para aclarar la relación entre el presente Reglamento y la Directiva 2002/58/CE, esta última debe ser modificada en consecuencia. Una vez que se adopte el presente Reglamento, debe revisarse la Directiva 2002/58/CE, en particular con objeto de garantizar la coherencia con el presente Reglamento.

HAN ADOPTADO EL PRESENTE REGLAMENTO

---

(1) DO C 229 de 31.7.2012, p. 90.

(2) DO C 391 de 18.12.2012, p. 127.

(3) Posición del Parlamento Europeo de 12 de marzo de 2014 (pendiente de publicación en el Diario Oficial) y posición del Consejo en primera lectura de 8 de abril de 2016 (pendiente de publicación en el Diario Oficial). Posición del Parlamento Europeo de 14 de abril de 2016.

(4) Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

(5) Recomendación de la Comisión de 6 de mayo de 2003 sobre la definición de microempresas, pequeñas y medianas empresas [C(2003) 1422] (DO L 124 de 20.5.2003, p. 36).

(6) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p. 1).

(7) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo (véase la página 89 del presente Diario Oficial).

(8) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1).

(9) Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88 de 4.4.2011, p. 45).

(10) Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores (DO L 95 de 21.4.1993, p. 29).

(11) Reglamento (CE) n.º 1338/2008 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo (DO L 354 de 31.12.2008, p. 70).

(12) Reglamento (UE) n.º 182/2011 del Parlamento Europeo y del Consejo, de 16 de febrero de 2011, por el que se establecen las normas y los principios generales relativos a las modalidades de control por parte de los Estados miembros del ejercicio de las competencias de ejecución por la Comisión (DO L 55 de 28.2.2011, p. 13).

(13) Reglamento (UE) n.º 1215/2012 del Parlamento Europeo y del Consejo, de 12 de diciembre de 2012, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 351 de 20.12.2012, p. 1).

(14) Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público (DO L 345 de 31.12.2003, p. 90).

(15) Reglamento (UE) n.º 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DO L 158 de 27.5.2014, p. 1).

(16) Reglamento (CE) n.º 223/2009 del Parlamento Europeo y del Consejo, de 11 de marzo de 2009, relativo a la estadística europea y por el que se deroga el Reglamento (CE, Euratom) n.º 1101/2008 relativo a la transmisión a la Oficina Estadística de las Comunidades Europeas de las informaciones amparadas por el secreto estadístico, el Reglamento (CE) n.º 322/97 del Consejo sobre la estadística comunitaria y la Decisión 89/382/CEE, Euratom del Consejo por la que se crea un Comité del programa estadístico de las Comunidades Europeas (DO L 87 de 31.3.2009, p. 164).

(17) DO C 192 de 30.6.2012, p. 7.

(18) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37).

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos.

2. El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales.

3. La libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Artículo 2. *Ámbito de aplicación material.*

1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

2. El presente Reglamento no se aplica al tratamiento de datos personales:

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;

c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

3. El Reglamento (CE) n.º 45/2001 es de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión. El Reglamento (CE) n.º 45/2001 y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98.

4. El presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15.

Artículo 3. *Ámbito territorial.*

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que se encuentren en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público.

Artículo 4. *Definiciones.*

A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o

cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

3) «limitación del tratamiento»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro;

4) «elaboración de perfiles»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física;

5) «seudonimización»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable;

6) «fichero»: todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

9) «destinatario»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

10) «tercero»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

11) «consentimiento del interesado»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;

12) «violación de la seguridad de los datos personales»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos;

13) «datos genéticos»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

15) «datos relativos a la salud»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

16) «establecimiento principal»:

a) en lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las

decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal;

b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento;

17) «representante»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento;

18) «empresa»: persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

19) «grupo empresarial»: grupo constituido por una empresa que ejerce el control y sus empresas controladas;

20) «normas corporativas vinculantes»: las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

21) «autoridad de control»: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

22) «autoridad de control interesada»: la autoridad de control a la que afecta el tratamiento de datos personales debido a que:

a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control;

b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o

c) se ha presentado una reclamación ante esa autoridad de control;

23) «tratamiento transfronterizo»:

a) el tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o

b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

24) «objeción pertinente y motivada»: la objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

25) «servicio de la sociedad de la información»: todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo [(19)];

26) «organización internacional»: una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

---

(19) Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1).

CAPÍTULO II

Principios

Artículo 5. *Principios relativos al tratamiento.*

1. Los datos personales serán:

a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);

e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

Artículo 6. *Licitud del tratamiento.*

1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;

c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no

prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

a) el Derecho de la Unión, o

b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:

a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;

b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;

c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;

d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;

e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.

Artículo 7. *Condiciones para el consentimiento.*

1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.

3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el

consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.

Artículo 8. *Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información.*

1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años.

2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.

3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño.

Artículo 9. *Tratamiento de categorías especiales de datos personales.*

1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Artículo 10. *Tratamiento de datos personales relativos a condenas e infracciones penales.*

El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.

Artículo 11. *Tratamiento que no requiere identificación.*

1. Si los fines para los cuales un responsable trata datos personales no requieren o ya no requieren la identificación de un interesado por el responsable, este no estará obligado a mantener, obtener o tratar información adicional con vistas a identificar al interesado con la única finalidad de cumplir el presente Reglamento.

2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.

CAPÍTULO III

Derechos del interesado

Sección 1. Transparencia y modalidades

Artículo 12. *Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado.*

1. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.

2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.

3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, sin dilación indebida y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.

4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.

5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:

a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o

b) negarse a actuar respecto de la solicitud.

El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud.

6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.

7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.

8. La Comisión estará facultada para adoptar actos delegados de conformidad con el artículo 92 a fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

Sección 2. Información y acceso a los datos personales

Artículo 13. *Información que deberá facilitarse cuando los datos personales se obtengan del interesado.*

1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.
4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Artículo 14. *Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado.*

1. Cuando los datos personales no se hayan obtenido del interesado, el responsable del tratamiento le facilitará la siguiente información:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;

d) las categorías de datos personales de que se trate;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:

a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;

b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;

c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;

e) el derecho a presentar una reclamación ante una autoridad de control;

f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;

g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:

a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;

b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o

c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.

5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:

a) el interesado ya disponga de la información;

b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;

c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o

d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza legal.

Artículo 15. *Derecho de acceso del interesado.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

a) los fines del tratamiento;

b) las categorías de datos personales de que se trate;

c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros países u organizaciones internacionales;

d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;

e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;

f) el derecho a presentar una reclamación ante una autoridad de control;

g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;

h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.

3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.

4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.

Sección 3. Rectificación y supresión

Artículo 16. *Derecho de rectificación.*

El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Artículo 17. *Derecho de supresión («el derecho al olvido»).*

1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;

b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;

c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;

e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;

f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.

2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:

a) para ejercer el derecho a la libertad de expresión e información;

b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3;

d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o

e) para la formulación, el ejercicio o la defensa de reclamaciones.

Artículo 18. *Derecho a la limitación del tratamiento.*

1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales en un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.

Artículo 19. *Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.*

El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.

Artículo 20. *Derecho a la portabilidad de los datos.*

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:

a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y

b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.

3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Sección 4. Derecho de oposición y decisiones individuales automatizadas

Artículo 21. *Derecho de oposición.*

1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.

3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.

4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.

Artículo 22. *Decisiones individuales automatizadas, incluida la elaboración de perfiles.*

1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

2. El apartado 1 no se aplicará si la decisión:

a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;

b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o

c) se basa en el consentimiento explícito del interesado.

3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Sección 5. Limitaciones

Artículo 23. *Limitaciones.*

1. El Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar:

a) la seguridad del Estado;

b) la defensa;

c) la seguridad pública;

d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención;

e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social;

f) la protección de la independencia judicial y de los procedimientos judiciales;

g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas;

h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g);

i) la protección del interesado o de los derechos y libertades de otros;

j) la ejecución de demandas civiles.

2. En particular, cualquier medida legislativa indicada en el apartado 1 contendrá como mínimo, en su caso, disposiciones específicas relativas a:

a) la finalidad del tratamiento o de las categorías de tratamiento;

b) las categorías de datos personales de que se trate;

c) el alcance de las limitaciones establecidas;

d) las garantías para evitar accesos o transferencias ilícitos o abusivos;

e) la determinación del responsable o de categorías de responsables;

f) los plazos de conservación y las garantías aplicables habida cuenta de la naturaleza, alcance y objetivos del tratamiento o las categorías de tratamiento;

g) los riesgos para los derechos y libertades de los interesados, y

h) el derecho de los interesados a ser informados sobre la limitación, salvo si puede ser perjudicial a los fines de esta.

CAPÍTULO IV

Responsable del tratamiento y encargado del tratamiento

Sección 1. Obligaciones generales

Artículo 24. *Responsabilidad del responsable del tratamiento.*

1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.

2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.

3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

Artículo 25. *Protección de datos desde el diseño y por defecto.*

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Artículo 26. *Corresponsables del tratamiento.*

1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados

miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.

2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.

3. Independientemente de los términos del acuerdo a que se refiere el apartado 1, los interesados podrán ejercer los derechos que les reconoce el presente Reglamento frente a, y en contra de, cada uno de los responsables.

Artículo 27. *Representantes de responsables o encargados del tratamiento no establecidos en la Unión.*

1. Cuando sea de aplicación el artículo 3, apartado 2, el responsable o el encargado del tratamiento designará por escrito un representante en la Unión.

2. La obligación establecida en el apartado 1 del presente artículo no será aplicable:

a) al tratamiento que sea ocasional, que no incluyan el manejo a gran escala de categorías especiales de datos indicadas en el artículo 9, apartado 1, o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, y que sea improbable que entrañe un riesgo para los derechos y libertades de las personas físicas, teniendo en cuenta la naturaleza, contexto, alcance y objetivos del tratamiento, o

b) a las autoridades u organismos públicos.

3. El representante estará establecido en uno de los Estados miembros en que estén los interesados cuyos datos personales se traten en el contexto de una oferta de bienes o servicios, o cuyo comportamiento esté siendo controlado.

4. El responsable o el encargado del tratamiento encomendará al representante que atienda, junto al responsable o al encargado, o en su lugar, a las consultas, en particular, de las autoridades de control y de los interesados, sobre todos los asuntos relativos al tratamiento, a fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento.

5. La designación de un representante por el responsable o el encargado del tratamiento se entenderá sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable o encargado.

Artículo 28. *Encargado del tratamiento.*

1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;

b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;

c) tomará todas las medidas necesarias de conformidad con el artículo 32;

d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;

f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;

g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;

h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Artículo 29. *Tratamiento bajo la autoridad del responsable o del encargado del tratamiento.*

El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 30. *Registro de las actividades de tratamiento.*

1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;
b) las categorías de tratamientos efectuados por cuenta de cada responsable;
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.
4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.
5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

Artículo 31. *Cooperación con la autoridad de control.*

El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.

Sección 2. Seguridad de los datos personales

Artículo 32. *Seguridad del tratamiento.*

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.
4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

Artículo 33. *Notificación de una violación de la seguridad de los datos personales a la autoridad de control.*

1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.

Artículo 34. *Comunicación de una violación de la seguridad de los datos personales al interesado.*

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.

Sección 3. Evaluación de impacto relativa a la protección de datos y consulta previa

Artículo 35. *Evaluación de impacto relativa a la protección de datos.*

1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o

c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.

Artículo 36. *Consulta previa.*

1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.

2. Cuando la autoridad de control considere que el tratamiento previsto a que se refiere el apartado 1 podría infringir el presente Reglamento, en particular cuando el responsable no

haya identificado o mitigado suficientemente el riesgo, la autoridad de control deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable, y en su caso al encargado, y podrá utilizar cualquiera de sus poderes mencionados en el artículo 58. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable y, en su caso, al encargado de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:

a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;

b) los fines y medios del tratamiento previsto;

c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;

d) en su caso, los datos de contacto del delegado de protección de datos;

e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y

f) cualquier otra información que solicite la autoridad de control.

4. Los Estados miembros garantizarán que se consulte a la autoridad de control durante la elaboración de toda propuesta de medida legislativa que haya de adoptar un Parlamento nacional, o de una medida reglamentaria basada en dicha medida legislativa, que se refiera al tratamiento.

5. No obstante lo dispuesto en el apartado 1, el Derecho de los Estados miembros podrá obligar a los responsables del tratamiento a consultar a la autoridad de control y a recabar su autorización previa en relación con el tratamiento por un responsable en el ejercicio de una misión realizada en interés público, en particular el tratamiento en relación con la protección social y la salud pública.

Sección 4. Delegado de protección de datos

Artículo 37. *Designación del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10.

2. Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

3. Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.

4. En casos distintos de los contemplados en el apartado 1, el responsable o el encargado del tratamiento o las asociaciones y otros organismos que representen a categorías de responsables o encargados podrán designar un delegado de protección de datos o deberán designarlo si así lo exige el Derecho de la Unión o de los Estados miembros. El delegado de protección de datos podrá actuar por cuenta de estas asociaciones y otros organismos que representen a responsables o encargados.

5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Artículo 38. *Posición del delegado de protección de datos.*

1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.

2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.

3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.

4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.

5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.

6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.

Artículo 39. *Funciones del delegado de protección de datos.*

1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:

a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;

b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;

d) cooperar con la autoridad de control;

e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.

2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

Sección 5. Códigos de conducta y certificación

Artículo 40. *Códigos de conducta.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación del presente Reglamento, teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Las asociaciones y otros organismos representativos de categorías de responsables o encargados del tratamiento podrán elaborar códigos de conducta o modificar o ampliar dichos códigos con objeto de especificar la aplicación del presente Reglamento, como en lo que respecta a:

a) el tratamiento leal y transparente;

b) los intereses legítimos perseguidos por los responsables del tratamiento en contextos específicos;

c) la recogida de datos personales;

d) la seudonimización de datos personales;

e) la información proporcionada al público y a los interesados;

f) el ejercicio de los derechos de los interesados;

g) la información proporcionada a los niños y la protección de estos, así como la manera de obtener el consentimiento de los titulares de la patria potestad o tutela sobre el niño;

h) las medidas y procedimientos a que se refieren los artículos 24 y 25 y las medidas para garantizar la seguridad del tratamiento a que se refiere el artículo 32;

i) la notificación de violaciones de la seguridad de los datos personales a las autoridades de control y la comunicación de dichas violaciones a los interesados;

j) la transferencia de datos personales a terceros países u organizaciones internacionales, o

k) los procedimientos extrajudiciales y otros procedimientos de resolución de conflictos que permitan resolver las controversias entre los responsables del tratamiento y los interesados relativas al tratamiento, sin perjuicio de los derechos de los interesados en virtud de los artículos 77 y 79.

3. Además de la adhesión de los responsables o encargados del tratamiento a los que se aplica el presente Reglamento, los responsables o encargados a los que no se aplica el presente Reglamento en virtud del artículo 3 podrán adherirse también a códigos de conducta aprobados de conformidad con el apartado 5 del presente artículo y que tengan validez general en virtud del apartado 9 del presente artículo, a fin de ofrecer garantías adecuadas en el marco de las transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra e). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

4. El código de conducta a que se refiere el apartado 2 del presente artículo contendrá mecanismos que permitan al organismo mencionado en el artículo 41, apartado 1, efectuar el control obligatorio del cumplimiento de sus disposiciones por los responsables o encargados de tratamiento que se comprometan a aplicarlo, sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes con arreglo al artículo 51 o 56.

5. Las asociaciones y otros organismos mencionados en el apartado 2 del presente artículo que proyecten elaborar un código de conducta o modificar o ampliar un código existente presentarán el proyecto de código o la modificación o ampliación a la autoridad de control que sea competente con arreglo al artículo 55. La autoridad de control dictaminará si el proyecto de código o la modificación o ampliación es conforme con el presente Reglamento y aprobará dicho proyecto de código, modificación o ampliación si considera suficientes las garantías adecuadas ofrecidas.

6. Si el proyecto de código o la modificación o ampliación es aprobado de conformidad con el apartado 5 y el código de conducta de que se trate no se refiere a actividades de

tratamiento en varios Estados miembros, la autoridad de control registrará y publicará el código.

7. Si un proyecto de código de conducta guarda relación con actividades de tratamiento en varios Estados miembros, la autoridad de control que sea competente en virtud del artículo 55 lo presentará por el procedimiento mencionado en el artículo 63, antes de su aprobación o de la modificación o ampliación, al Comité, el cual dictaminará si dicho proyecto, modificación o ampliación es conforme con el presente Reglamento o, en la situación indicada en el apartado 3 del presente artículo, ofrece garantías adecuadas.

8. Si el dictamen a que se refiere el apartado 7 confirma que el proyecto de código o la modificación o ampliación cumple lo dispuesto en el presente Reglamento o, en la situación indicada en el apartado 3, ofrece garantías adecuadas, el Comité presentará su dictamen a la Comisión.

9. La Comisión podrá, mediante actos de ejecución, decidir que el código de conducta o la modificación o ampliación aprobados y presentados con arreglo al apartado 8 del presente artículo tengan validez general dentro de la Unión. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

10. La Comisión dará publicidad adecuada a los códigos aprobados cuya validez general haya sido decidida de conformidad con el apartado 9.

11. El Comité archivará en un registro todos los códigos de conducta, modificaciones y ampliaciones que se aprueben, y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 41. *Supervisión de códigos de conducta aprobados.*

1. Sin perjuicio de las funciones y los poderes de la autoridad de control competente en virtud de los artículos 57 y 58, podrá supervisar el cumplimiento de un código de conducta en virtud del artículo 40 un organismo que tenga el nivel adecuado de pericia en relación con el objeto del código y que haya sido acreditado para tal fin por la autoridad de control competente.

2. El organismo a que se refiere el apartado 1 podrá ser acreditado para supervisar el cumplimiento de un código de conducta si:

a) ha demostrado, a satisfacción de la autoridad de control competente, su independencia y pericia en relación con el objeto del código;

b) ha establecido procedimientos que le permitan evaluar la idoneidad de los responsables y encargados correspondientes para aplicar el código, supervisar el cumplimiento de sus disposiciones y examinar periódicamente su aplicación;

c) ha establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones del código o a la manera en que el código haya sido o esté siendo aplicado por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

d) ha demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La autoridad de control competente someterá al Comité, con arreglo al mecanismo de coherencia a que se refiere el artículo 63, el proyecto que fije los requisitos de acreditación de un organismo a que se refiere el apartado 1 del presente artículo.

4. Sin perjuicio de las funciones y los poderes de la autoridad de control competente y de lo dispuesto en el capítulo VIII, un organismo a tenor del apartado 1 del presente artículo deberá, con sujeción a garantías adecuadas, tomar las medidas oportunas en caso de infracción del código por un responsable o encargado del tratamiento, incluida la suspensión o exclusión de este. Informará de dichas medidas y de las razones de las mismas a la autoridad de control competente.

5. La autoridad de control competente revocará la acreditación de un organismo a tenor del apartado 1 si los requisitos de acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo infringe el presente Reglamento.

6. El presente artículo no se aplicará al tratamiento realizado por autoridades y organismos públicos.

Artículo 42. *Certificación.*

1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados.

3. La certificación será voluntaria y estará disponible a través de un proceso transparente.

4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56.

5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos.

6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación.

7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los criterios pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los criterios para la certificación.

8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado.

Artículo 43. *Organismo de certificación.*

1. Sin perjuicio de las funciones y poderes de la autoridad de control competente en virtud de los artículos 57 y 58, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos expedirán y renovarán las certificaciones una vez informada la autoridad de control, a fin de esta que pueda ejercer, si así se requiere, sus poderes en virtud del artículo 58, apartado 2, letra h). Los Estados miembros garantizarán que dichos organismos de certificación sean acreditados por la autoridad o el organismo indicado a continuación, o por ambos:

a) la autoridad de control que sea competente en virtud del artículo 55 o 56;

b) el organismo nacional de acreditación designado de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo [20] con arreglo a la norma EN ISO/IEC 17065/2012 y a los requisitos adicionales establecidos por la autoridad de control que sea competente en virtud del artículo 55 o 56.

2. Los organismos de certificación mencionados en el apartado 1 únicamente serán acreditados de conformidad con dicho apartado si:

a) han demostrado, a satisfacción de la autoridad de control competente, su independencia y su pericia en relación con el objeto de la certificación;

b) se han comprometido a respetar los criterios mencionados en el artículo 42, apartado 5, y aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56, o por el Comité de conformidad con el artículo 63;

c) han establecido procedimientos para la expedición, la revisión periódica y la retirada de certificaciones, sellos y marcas de protección de datos;

d) han establecido procedimientos y estructuras para tratar las reclamaciones relativas a infracciones de la certificación o a la manera en que la certificación haya sido o esté siendo aplicada por un responsable o encargado del tratamiento, y para hacer dichos procedimientos y estructuras transparentes para los interesados y el público, y

e) han demostrado, a satisfacción de la autoridad de control competente, que sus funciones y cometidos no dan lugar a conflicto de intereses.

3. La acreditación de los organismos de certificación a que se refieren los apartados 1 y 2 del presente artículo se realizará sobre la base de los requisitos aprobados por la autoridad de control que sea competente en virtud del artículo 55 o 56 o por el Comité en virtud del artículo 63. En caso de acreditación de conformidad con el apartado 1, letra b), del presente artículo, estos requisitos complementarán los contemplados en el Reglamento (CE) n.º 765/2008 y las normas técnicas que describen los métodos y procedimientos de los organismos de certificación.

4. Los organismos de certificación a que se refiere el apartado 1 serán responsable de la correcta evaluación a efectos de certificación o retirada de la certificación, sin perjuicio de la responsabilidad del responsable o del encargado del tratamiento en cuanto al cumplimiento del presente Reglamento. La acreditación se expedirá por un período máximo de cinco años y podrá ser renovada en las mismas condiciones, siempre y cuando el organismo de certificación cumpla los requisitos establecidos en el presente artículo.

5. Los organismos de certificación a que se refiere el apartado 1 comunicarán a las autoridades de control competentes las razones de la expedición de la certificación solicitada o de su retirada.

6. La autoridad de control hará públicos los requisitos a que se refiere el apartado 3 del presente artículo y los criterios a que se refiere el artículo 42, apartado 5, en una forma fácilmente accesible. Las autoridades de control comunicarán también dichos requisitos y criterios al Comité.

7. No obstante lo dispuesto en el capítulo VIII, la autoridad de control competente o el organismo nacional de acreditación revocará la acreditación a un organismo de certificación a tenor del apartado 1 del presente artículo si las condiciones de la acreditación no se cumplen o han dejado de cumplirse, o si la actuación de dicho organismo de certificación infringe el presente Reglamento.

8. La Comisión estará facultada para adoptar actos delegados, de conformidad con el artículo 92, a fin de especificar las condiciones que deberán tenerse en cuenta para los mecanismos de certificación en materia de protección de datos a que se refiere el artículo 42, apartado 1.

9. La Comisión podrá adoptar actos de ejecución que establezcan normas técnicas para los mecanismos de certificación y los sellos y marcas de protección de datos, y mecanismos para promover y reconocer dichos mecanismos de certificación, sellos y marcas. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

---

[20] Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93 (DO L 218 de 13.8.2008, p. 30).

CAPÍTULO V

Transferencias de datos personales a terceros países u organizaciones internacionales

Artículo 44. *Principio general de las transferencias.*

Solo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si, a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional. Todas las disposiciones del presente capítulo se aplicarán a fin de asegurar que el nivel de protección de las personas físicas garantizado por el presente Reglamento no se vea menoscabado.

Artículo 45. *Transferencias basadas en una decisión de adecuación.*

1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

2. Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

3. La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control a que se refiere el apartado 2, letra b), del presente artículo. El acto de ejecución se adoptará con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

4. La Comisión supervisará de manera continuada los acontecimientos en países terceros y organizaciones internacionales que puedan afectar a la efectiva aplicación de las

decisiones adoptadas con arreglo al apartado 3 del presente artículo y de las decisiones adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE.

5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

Por razones imperiosas de urgencia debidamente justificadas, la Comisión adoptará actos de ejecución inmediatamente aplicables de conformidad con el procedimiento a que se refiere el artículo 93, apartado 3.

6 La Comisión entablará consultas con el tercer país u organización internacional con vistas a poner remedio a la situación que dé lugar a la decisión adoptada de conformidad con el apartado 5.

7. Toda decisión de conformidad con el apartado 5 del presente artículo se entenderá sin perjuicio de las transferencias de datos personales al tercer país, a un territorio o uno o varios sectores específicos de ese tercer país, o a la organización internacional de que se trate en virtud de los artículos 46 a 49.

8. La Comisión publicará en el Diario Oficial de la Unión Europea y en su página web una lista de terceros países, territorios y sectores específicos en un tercer país, y organizaciones internacionales respecto de los cuales haya decidido que se garantiza, o ya no, un nivel de protección adecuado.

9. Las decisiones adoptadas por la Comisión en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas por una decisión de la Comisión adoptada de conformidad con los apartados 3 o 5 del presente artículo.

Artículo 46. *Transferencias mediante garantías adecuadas.*

1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:

a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;

b) normas corporativas vinculantes de conformidad con el artículo 47;

c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;

d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;

e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o

f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o

b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.

4. La autoridad de control aplicará el mecanismo de coherencia a que se refiere el artículo 63 en los casos indicados en el apartado 3 del presente artículo.

5. Las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad con el artículo 26, apartado 2, de la Directiva 95/46/CE seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, en caso necesario, por dicha autoridad de control. Las decisiones adoptadas por la Comisión en virtud del artículo 26, apartado 4, de la Directiva 95/46/CE permanecerán en vigor hasta que sean modificadas, sustituidas o derogadas, en caso necesario, por una decisión de la Comisión adoptada de conformidad con el apartado 2 del presente artículo.

Artículo 47. *Normas corporativas vinculantes.*

1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:

a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;

b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y

c) cumplan los requisitos establecidos en el apartado 2.

2. Las normas corporativas vinculantes mencionadas en el apartado 1 especificarán, como mínimo, los siguientes elementos:

a) la estructura y los datos de contacto del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta y de cada uno de sus miembros;

b) las transferencias o conjuntos de transferencias de datos, incluidas las categorías de datos personales, el tipo de tratamientos y sus fines, el tipo de interesados afectados y el nombre del tercer o los terceros países en cuestión;

c) su carácter jurídicamente vinculante, tanto a nivel interno como externo;

d) la aplicación de los principios generales en materia de protección de datos, en particular la limitación de la finalidad, la minimización de los datos, los periodos de conservación limitados, la calidad de los datos, la protección de los datos desde el diseño y por defecto, la base del tratamiento, el tratamiento de categorías especiales de datos personales, las medidas encaminadas a garantizar la seguridad de los datos y los requisitos con respecto a las transferencias ulteriores a organismos no vinculados por las normas corporativas vinculantes;

e) los derechos de los interesados en relación con el tratamiento y los medios para ejercerlos, en particular el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, incluida la elaboración de perfiles de conformidad con lo dispuesto en el artículo 22, el derecho a presentar una reclamación ante la autoridad de control competente y ante los tribunales competentes de los Estados miembros de conformidad con el artículo 79, y el derecho a obtener una reparación, y, cuando proceda, una indemnización por violación de las normas corporativas vinculantes;

f) la aceptación por parte del responsable o del encargado del tratamiento establecidos en el territorio de un Estado miembro de la responsabilidad por cualquier violación de las normas corporativas vinculantes por parte de cualquier miembro de que se trate no establecido en la Unión; el responsable o el encargado solo será exonerado, total o parcialmente, de dicha responsabilidad si demuestra que el acto que originó los daños y perjuicios no es imputable a dicho miembro;

g) la forma en que se facilita a los interesados la información sobre las normas corporativas vinculantes, en particular en lo que respecta a las disposiciones contempladas en las letras d), e) y f) del presente apartado, además de los artículos 13 y 14;

h) las funciones de todo delegado de protección de datos designado de conformidad con el artículo 37, o de cualquier otra persona o entidad encargada de la supervisión del cumplimiento de las normas corporativas vinculantes dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, así como de la supervisión de la formación y de la tramitación de las reclamaciones;

i) los procedimientos de reclamación;

j) los mecanismos establecidos dentro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta para garantizar la verificación del cumplimiento de las normas corporativas vinculantes. Dichos mecanismos incluirán auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del interesado. Los resultados de dicha verificación deberían comunicarse a la persona o entidad a que se refiere la letra h) y al consejo de administración de la empresa que controla un grupo empresarial, o de la unión de empresas dedicadas a una actividad económica conjunta, y ponerse a disposición de la autoridad de control competente que lo solicite;

k) los mecanismos establecidos para comunicar y registrar las modificaciones introducidas en las normas y para notificar esas modificaciones a la autoridad de control;

l) el mecanismo de cooperación con la autoridad de control para garantizar el cumplimiento por parte de cualquier miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, en particular poniendo a disposición de la autoridad de control los resultados de las verificaciones de las medidas contempladas en la letra j);

m) los mecanismos para informar a la autoridad de control competente de cualquier requisito jurídico de aplicación en un país tercero a un miembro del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, que probablemente tengan un efecto adverso sobre las garantías establecidas en las normas corporativas vinculantes, y

n) la formación en protección de datos pertinente para el personal que tenga acceso permanente o habitual a datos personales.

3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 48. *Transferencias o comunicaciones no autorizadas por el Derecho de la Unión.*

Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.

Artículo 49. *Excepciones para situaciones específicas.*

1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:

a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;

b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.

Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos.

2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.

3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.

4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.

5. En ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el Derecho de la Unión o de los Estados miembros podrá, por razones importantes de interés público, establecer expresamente límites a la transferencia de categorías específicas de datos a un tercer país u organización internacional. Los Estados miembros notificarán a la Comisión dichas disposiciones.

6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.

Artículo 50. *Cooperación internacional en el ámbito de la protección de datos personales.*

En relación con los terceros países y las organizaciones internacionales, la Comisión y las autoridades de control tomarán medidas apropiadas para:

a) crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos personales;

b) prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías adecuadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) asociar a partes interesadas en la materia a los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) promover el intercambio y la documentación de la legislación y las prácticas en materia de protección de datos personales, inclusive en materia de conflictos de jurisdicción con terceros países.

CAPÍTULO VI

Autoridades de control independientes

Sección 1. Independencia

Artículo 51. *Autoridad de control.*

1. Cada Estado miembro establecerá que sea responsabilidad de una o varias autoridades públicas independientes (en adelante «autoridad de control») supervisar la aplicación del presente Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión.

2. Cada autoridad de control contribuirá a la aplicación coherente del presente Reglamento en toda la Unión. A tal fin, las autoridades de control cooperarán entre sí y con la Comisión con arreglo a lo dispuesto en el capítulo VII.

3. Cuando haya varias autoridades de control en un Estado miembro, este designará la autoridad de control que representará a dichas autoridades en el Comité, y establecerá el mecanismo que garantice el cumplimiento por las demás autoridades de las normas relativas al mecanismo de coherencia a que se refiere el artículo 63.

4. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el presente capítulo a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que afecte a dichas disposiciones.

Artículo 52. *Independencia.*

1. Cada autoridad de control actuará con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento.

2. El miembro o los miembros de cada autoridad de control serán ajenos, en el desempeño de sus funciones y en el ejercicio de sus poderes de conformidad con el presente Reglamento, a toda influencia externa, ya sea directa o indirecta, y no solicitarán ni admitirán ninguna instrucción.

3. El miembro o los miembros de cada autoridad de control se abstendrán de cualquier acción que sea incompatible con sus funciones y no participarán, mientras dure su mandato, en ninguna actividad profesional que sea incompatible, remunerada o no.

4. Cada Estado miembro garantizará que cada autoridad de control disponga en todo momento de los recursos humanos, técnicos y financieros, así como de los locales y las infraestructuras necesarios para el cumplimiento efectivo de sus funciones y el ejercicio de sus poderes, incluidos aquellos que haya de ejercer en el marco de la asistencia mutua, la cooperación y la participación en el Comité.

5. Cada Estado miembro garantizará que cada autoridad de control elija y disponga de su propio personal, que estará sujeto a la autoridad exclusiva del miembro o miembros de la autoridad de control interesada.

6. Cada Estado miembro garantizará que cada autoridad de control esté sujeta a un control financiero que no afecte a su independencia y que disponga de un presupuesto anual, público e independiente, que podrá formar parte del presupuesto general del Estado o de otro ámbito nacional.

Artículo 53. *Condiciones generales aplicables a los miembros de la autoridad de control.*

1. Los Estados miembros dispondrán que cada miembro de sus autoridades de control sea nombrado mediante un procedimiento transparente por:

— su Parlamento,
— su Gobierno,
— su Jefe de Estado, o
— un organismo independiente encargado del nombramiento en virtud del Derecho de los Estados miembros.

2. Cada miembro poseerá la titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales, necesarias para el cumplimiento de sus funciones y el ejercicio de sus poderes.

3. Los miembros darán por concluidas sus funciones en caso de terminación del mandato, dimisión o jubilación obligatoria, de conformidad con el Derecho del Estado miembro de que se trate.

4. Un miembro será destituido únicamente en caso de conducta irregular grave o si deja de cumplir las condiciones exigidas en el desempeño de sus funciones.

Artículo 54. *Normas relativas al establecimiento de la autoridad de control.*

1. Cada Estado miembro establecerá por ley todos los elementos indicados a continuación:

a) el establecimiento de cada autoridad de control;

b) las cualificaciones y condiciones de idoneidad necesarias para ser nombrado miembro de cada autoridad de control;

c) las normas y los procedimientos para el nombramiento del miembro o miembros de cada autoridad de control;

d) la duración del mandato del miembro o los miembros de cada autoridad de control, no inferior a cuatro años, salvo el primer nombramiento posterior al 24 de mayo de 2016, parte del cual podrá ser más breve cuando sea necesario para proteger la independencia de la autoridad de control por medio de un procedimiento de nombramiento escalonado;

e) el carácter renovable o no del mandato del miembro o los miembros de cada autoridad de control y, en su caso, el número de veces que podrá renovarse;

f) las condiciones por las que se rigen las obligaciones del miembro o los miembros y del personal de cada autoridad de control, las prohibiciones relativas a acciones, ocupaciones y prestaciones incompatibles con el cargo durante el mandato y después del mismo, y las normas que rigen el cese en el empleo.

2. El miembro o miembros y el personal de cada autoridad de control estarán sujetos, de conformidad con el Derecho de la Unión o de los Estados miembros, al deber de secreto profesional, tanto durante su mandato como después del mismo, con relación a las informaciones confidenciales de las que hayan tenido conocimiento en el cumplimiento de sus funciones o el ejercicio de sus poderes. Durante su mandato, dicho deber de secreto profesional se aplicará en particular a la información recibida de personas físicas en relación con infracciones del presente Reglamento.

Sección 2. Competencia, funciones y poderes

Artículo 55. *Competencia.*

1. Cada autoridad de control será competente para desempeñar las funciones que se le asignen y ejercer los poderes que se le confieran de conformidad con el presente Reglamento en el territorio de su Estado miembro.

2. Cuando el tratamiento sea efectuado por autoridades públicas o por organismos privados que actúen con arreglo al artículo 6, apartado 1, letras c) o e), será competente la autoridad de control del Estado miembro de que se trate. No será aplicable en tales casos el artículo 56.

3. Las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial.

Artículo 56. *Competencia de la autoridad de control principal.*

1. Sin perjuicio de lo dispuesto en el artículo 55, la autoridad de control del establecimiento principal o del único establecimiento del responsable o del encargado del tratamiento será competente para actuar como autoridad de control principal para el tratamiento transfronterizo realizado por parte de dicho responsable o encargado con arreglo al procedimiento establecido en el artículo 60.

2. No obstante lo dispuesto en el apartado 1, cada autoridad de control será competente para tratar una reclamación que le sea presentada o una posible infracción del presente Reglamento, en caso de que se refiera únicamente a un establecimiento situado en su Estado miembro o únicamente afecte de manera sustancial a interesados en su Estado miembro.

3. En los casos a que se refiere el apartado 2 del presente artículo, la autoridad de control informará sin dilación al respecto a la autoridad de control principal. En el plazo de tres semanas después de haber sido informada, la autoridad de control principal decidirá si tratará o no el caso de conformidad con el procedimiento establecido en el artículo 60, teniendo presente si existe un establecimiento del responsable o encargado del tratamiento en el Estado miembro de la autoridad de control que le haya informado.

4. En caso de que la autoridad de control principal decida tratar el caso, se aplicará el procedimiento establecido en el artículo 60. La autoridad de control que haya informado a la autoridad de control principal podrá presentarle un proyecto de decisión. La autoridad de control principal tendrá en cuenta en la mayor medida posible dicho proyecto al preparar el proyecto de decisión a que se refiere el artículo 60, apartado 3.

5. En caso de que la autoridad de control principal decida no tratar el caso, la autoridad de control que le haya informado lo tratará con arreglo a los artículos 61 y 62.

6. La autoridad de control principal será el único interlocutor del responsable o del encargado en relación con el tratamiento transfronterizo realizado por dicho responsable o encargado.

Artículo 57. *Funciones.*

1. Sin perjuicio de otras funciones en virtud del presente Reglamento, incumbirá a cada autoridad de control, en su territorio:

a) controlar la aplicación del presente Reglamento y hacerlo aplicar;

b) promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento. Las actividades dirigidas específicamente a los niños deberán ser objeto de especial atención;

c) asesorar, con arreglo al Derecho de los Estados miembros, al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento;

d) promover la sensibilización de los responsables y encargados del tratamiento acerca de las obligaciones que les incumben en virtud del presente Reglamento;

e) previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembros;

f) tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control;

g) cooperar, en particular compartiendo información, con otras autoridades de control y prestar asistencia mutua con el fin de garantizar la coherencia en la aplicación y ejecución del presente Reglamento;

h) llevar a cabo investigaciones sobre la aplicación del presente Reglamento, en particular basándose en información recibida de otra autoridad de control u otra autoridad pública;

i) hacer un seguimiento de cambios que sean de interés, en la medida en que tengan incidencia en la protección de datos personales, en particular el desarrollo de las tecnologías de la información y la comunicación y las prácticas comerciales;

j) adoptar las cláusulas contractuales tipo a que se refieren el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

k) elaborar y mantener una lista relativa al requisito de la evaluación de impacto relativa a la protección de datos, en virtud del artículo 35, apartado 4;

l) ofrecer asesoramiento sobre las operaciones de tratamiento contempladas en el artículo 36, apartado 2;

m) alentar la elaboración de códigos de conducta con arreglo al artículo 40, apartado 1, y dictaminar y aprobar los códigos de conducta que den suficientes garantías con arreglo al artículo 40, apartado 5;

n) fomentar la creación de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos con arreglo al artículo 42, apartado 1, y aprobar los criterios de certificación de conformidad con el artículo 42, apartado 5;

o) llevar a cabo, si procede, una revisión periódica de las certificaciones expedidas en virtud del artículo 42, apartado 7;

p) elaborar y publicar los requisitos para la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

q) efectuar la acreditación de organismos de supervisión de los códigos de conducta con arreglo al artículo 41 y de organismos de certificación con arreglo al artículo 43;

r) autorizar las cláusulas contractuales y disposiciones a que se refiere el artículo 46, apartado 3;

s) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47;

t) contribuir a las actividades del Comité;

u) llevar registros internos de las infracciones del presente Reglamento y de las medidas adoptadas de conformidad con el artículo 58, apartado 2, y

v) desempeñar cualquier otra función relacionada con la protección de los datos personales.

2. Cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación.

3. El desempeño de las funciones de cada autoridad de control será gratuito para el interesado y, en su caso, para el delegado de protección de datos.

4. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, la autoridad de control podrá establecer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de la solicitud. La carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud recaerá en la autoridad de control.

Artículo 58. *Poderes.*

1. Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación:

a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones;

b) llevar a cabo investigaciones en forma de auditorías de protección de datos;

c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7;

d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento;

e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones;

f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros.

2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

a) dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento;

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales;

f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;

g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;

h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación;

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

3. Cada autoridad de control dispondrá de todos los poderes de autorización y consultivos indicados a continuación:

a) asesorar al responsable del tratamiento conforme al procedimiento de consulta previa contemplado en el artículo 36;

b) emitir, por iniciativa propia o previa solicitud, dictámenes destinados al Parlamento nacional, al Gobierno del Estado miembro o, con arreglo al Derecho de los Estados miembros, a otras instituciones y organismos, así como al público, sobre cualquier asunto relacionado con la protección de los datos personales;

c) autorizar el tratamiento a que se refiere el artículo 36, apartado 5, si el Derecho del Estado miembro requiere tal autorización previa;

d) emitir un dictamen y aprobar proyectos de códigos de conducta de conformidad con lo dispuesto en el artículo 40, apartado 5;

e) acreditar los organismos de certificación con arreglo al artículo 43;

f) expedir certificaciones y aprobar criterios de certificación con arreglo al artículo 42, apartado 5;

g) adoptar las cláusulas tipo de protección de datos contempladas en el artículo 28, apartado 8, y el artículo 46, apartado 2, letra d);

h) autorizar las cláusulas contractuales indicadas en el artículo 46, apartado 3, letra a);

i) autorizar los acuerdos administrativos contemplados en el artículo 46, apartado 3, letra b);

j) aprobar normas corporativas vinculantes de conformidad con lo dispuesto en el artículo 47.

4. El ejercicio de los poderes conferidos a la autoridad de control en virtud del presente artículo estará sujeto a las garantías adecuadas, incluida la tutela judicial efectiva y al respeto de las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta.

5. Cada Estado miembro dispondrá por ley que su autoridad de control esté facultada para poner en conocimiento de las autoridades judiciales las infracciones del presente Reglamento y, si procede, para iniciar o ejercitar de otro modo acciones judiciales, con el fin de hacer cumplir lo dispuesto en el mismo.

6. Cada Estado miembro podrá establecer por ley que su autoridad de control tenga otros poderes además de los indicadas en los apartados 1, 2 y 3. El ejercicio de dichos poderes no será obstáculo a la aplicación efectiva del capítulo VII.

Artículo 59. *Informe de actividad.*

Cada autoridad de control elaborará un informe anual de sus actividades, que podrá incluir una lista de tipos de infracciones notificadas y de tipos de medidas adoptadas de conformidad con el artículo 58, apartado 2. Los informes se transmitirán al Parlamento nacional, al Gobierno y a las demás autoridades designadas en virtud del Derecho de los Estados miembros. Se pondrán a disposición del público, de la Comisión y del Comité.

CAPÍTULO VII

Cooperación y coherencia

Sección 1. Cooperación y coherencia

Artículo 60. *Cooperación entre la autoridad de control principal y las demás autoridades de control interesadas.*

1. La autoridad de control principal cooperará con las demás autoridades de control interesadas de acuerdo con el presente artículo, esforzándose por llegar a un consenso. La autoridad de control principal y las autoridades de control interesadas se intercambiarán toda información pertinente.

2. La autoridad de control principal podrá solicitar en cualquier momento a otras autoridades de control interesadas que presten asistencia mutua con arreglo al artículo 61, y podrá llevar a cabo operaciones conjuntas con arreglo al artículo 62, en particular para realizar investigaciones o supervisar la aplicación de una medida relativa a un responsable o un encargado del tratamiento establecido en otro Estado miembro.

3. La autoridad de control principal comunicará sin dilación a las demás autoridades de control interesadas la información pertinente a este respecto. Transmitirá sin dilación un proyecto de decisión a las demás autoridades de control interesadas para obtener su dictamen al respecto y tendrá debidamente en cuenta sus puntos de vista.

4. En caso de que cualquiera de las autoridades de control interesadas formule una objeción pertinente y motivada acerca del proyecto de decisión en un plazo de cuatro semanas a partir de la consulta con arreglo al apartado 3 del presente artículo, la autoridad de control principal someterá el asunto, en caso de que no siga lo indicado en la objeción pertinente y motivada o estime que dicha objeción no es pertinente o no está motivada, al mecanismo de coherencia contemplado en el artículo 63.

5. En caso de que la autoridad de control principal prevea seguir lo indicado en la objeción pertinente y motivada recibida, presentará a dictamen de las demás autoridades de control interesadas un proyecto de decisión revisado. Dicho proyecto de decisión revisado se someterá al procedimiento indicado en el apartado 4 en un plazo de dos semanas.

6. En caso de que ninguna otra autoridad de control interesada haya presentado objeciones al proyecto de decisión transmitido por la autoridad de control principal en el plazo indicado en los apartados 4 y 5, se considerará que la autoridad de control principal y

las autoridades de control interesadas están de acuerdo con dicho proyecto de decisión y estarán vinculadas por este.

7. La autoridad de control principal adoptará y notificará la decisión al establecimiento principal o al establecimiento único del responsable o el encargado del tratamiento, según proceda, e informará de la decisión a las autoridades de control interesadas y al Comité, incluyendo un resumen de los hechos pertinentes y la motivación. La autoridad de control ante la que se haya presentado una reclamación informará de la decisión al reclamante.

8. No obstante lo dispuesto en el apartado 7, cuando se desestime o rechace una reclamación, la autoridad de control ante la que se haya presentado adoptará la decisión, la notificará al reclamante e informará de ello al responsable del tratamiento.

9. En caso de que la autoridad de control principal y las autoridades de control interesadas acuerden desestimar o rechazar determinadas partes de una reclamación y atender otras partes de ella, se adoptará una decisión separada para cada una de esas partes del asunto. La autoridad de control principal adoptará la decisión respecto de la parte referida a acciones en relación con el responsable del tratamiento, la notificará al establecimiento principal o al único establecimiento del responsable o del encargado en el territorio de su Estado miembro, e informará de ello al reclamante, mientras que la autoridad de control del reclamante adoptará la decisión respecto de la parte relativa a la desestimación o rechazo de dicha reclamación, la notificará a dicho reclamante e informará de ello al responsable o al encargado.

10. Tras recibir la notificación de la decisión de la autoridad de control principal con arreglo a los apartados 7 y 9, el responsable o el encargado del tratamiento adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en lo tocante a las actividades de tratamiento en el contexto de todos sus establecimientos en la Unión. El responsable o el encargado notificarán las medidas adoptadas para dar cumplimiento a dicha decisión a la autoridad de control principal, que a su vez informará a las autoridades de control interesadas.

11. En circunstancias excepcionales, cuando una autoridad de control interesada tenga motivos para considerar que es urgente intervenir para proteger los intereses de los interesados, se aplicará el procedimiento de urgencia a que se refiere el artículo 66.

12. La autoridad de control principal y las demás autoridades de control interesadas se facilitarán recíprocamente la información requerida en el marco del presente artículo por medios electrónicos, utilizando un formulario normalizado.

Artículo 61. *Asistencia mutua.*

1. Las autoridades de control se facilitarán información útil y se prestarán asistencia mutua a fin de aplicar el presente Reglamento de manera coherente, y tomarán medidas para asegurar una efectiva cooperación entre ellas. La asistencia mutua abarcará, en particular, las solicitudes de información y las medidas de control, como las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

2. Cada autoridad de control adoptará todas las medidas oportunas requeridas para responder a una solicitud de otra autoridad de control sin dilación indebida y a más tardar en el plazo de un mes a partir de la solicitud. Dichas medidas podrán incluir, en particular, la transmisión de información pertinente sobre el desarrollo de una investigación.

3. Las solicitudes de asistencia deberán contener toda la información necesaria, entre otras cosas respecto de la finalidad y los motivos de la solicitud. La información que se intercambie se utilizará únicamente para el fin para el que haya sido solicitada.

4. La autoridad de control requerida no podrá negarse a responder a una solicitud, salvo si:

a) no es competente en relación con el objeto de la solicitud o con las medidas cuya ejecución se solicita, o

b) el hecho de responder a la solicitud infringiría el presente Reglamento o el Derecho de la Unión o de los Estados miembros que se aplique a la autoridad de control a la que se dirigió la solicitud.

5. La autoridad de control requerida informará a la autoridad de control requirente de los resultados obtenidos o, en su caso, de los progresos registrados o de las medidas

adoptadas para responder a su solicitud. La autoridad de control requerida explicará los motivos de su negativa a responder a una solicitud al amparo del apartado 4.

6. Como norma general, las autoridades de control requeridas facilitarán la información solicitada por otras autoridades de control por medios electrónicos, utilizando un formato normalizado.

7. Las autoridades de control requeridas no cobrarán tasa alguna por las medidas adoptadas a raíz de una solicitud de asistencia mutua. Las autoridades de control podrán convenir normas de indemnización recíproca por gastos específicos derivados de la prestación de asistencia mutua en circunstancias excepcionales.

8. Cuando una autoridad de control no facilite la información mencionada en el apartado 5 del presente artículo en el plazo de un mes a partir de la recepción de la solicitud de otra autoridad de control, la autoridad de control requirente podrá adoptar una medida provisional en el territorio de su Estado miembro de conformidad con lo dispuesto en el artículo 55, apartado 1. En ese caso, se supondrá que existe la necesidad urgente contemplada en el artículo 66, apartado 1, que exige una decisión urgente y vinculante del Comité en virtud del artículo 66, apartado 2.

9. La Comisión podrá, mediante actos de ejecución, especificar el formato y los procedimientos de asistencia mutua contemplados en el presente artículo, así como las modalidades del intercambio de información por medios electrónicos entre las autoridades de control y entre las autoridades de control y el Comité, en especial el formato normalizado mencionado en el apartado 6 del presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Artículo 62. *Operaciones conjuntas de las autoridades de control.*

1. Las autoridades de control realizarán, en su caso, operaciones conjuntas, incluidas investigaciones conjuntas y medidas de ejecución conjuntas, en las que participen miembros o personal de las autoridades de control de otros Estados miembros.

2. Si el responsable o el encargado del tratamiento tiene establecimientos en varios Estados miembros o si es probable que un número significativo de interesados en más de un Estado miembro se vean sustancialmente afectados por las operaciones de tratamiento, una autoridad de control de cada uno de esos Estados miembros tendrá derecho a participar en operaciones conjuntas. La autoridad de control que sea competente en virtud del artículo 56, apartados 1 o 4, invitará a la autoridad de control de cada uno de dichos Estados miembros a participar en las operaciones conjuntas y responderá sin dilación a la solicitud de participación presentada por una autoridad de control.

3. Una autoridad de control podrá, con arreglo al Derecho de su Estado miembro y con la autorización de la autoridad de control de origen, conferir poderes, incluidos poderes de investigación, a los miembros o al personal de la autoridad de control de origen que participen en operaciones conjuntas, o aceptar, en la medida en que lo permita el Derecho del Estado miembro de la autoridad de control de acogida, que los miembros o el personal de la autoridad de control de origen ejerzan sus poderes de investigación de conformidad con el Derecho del Estado miembro de la autoridad de control de origen. Dichos poderes de investigación solo podrán ejercerse bajo la orientación y en presencia de miembros o personal de la autoridad de control de acogida. Los miembros o el personal de la autoridad de control de origen estarán sujetos al Derecho del Estado miembro de la autoridad de control de acogida.

4. Cuando participe, de conformidad con el apartado 1, personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas.

5. El Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes.

6. Sin perjuicio del ejercicio de sus derechos frente a terceros y habida cuenta de la excepción establecida en el apartado 5, los Estados miembros renunciarán, en el caso contemplado en el apartado 1, a solicitar de otro Estado miembro el reembolso del importe de los daños y perjuicios mencionados en el apartado 4.

7. Cuando se prevea una operación conjunta y una autoridad de control no cumpla en el plazo de un mes con la obligación establecida en el apartado 2, segunda frase, del presente artículo, las demás autoridades de control podrán adoptar una medida provisional en el territorio de su Estado miembro de conformidad con el artículo 55. En ese caso, se presumirá la existencia de una necesidad urgente a tenor del artículo 66, apartado 1, y se requerirá dictamen o decisión vinculante urgente del Comité en virtud del artículo 66, apartado 2.

Sección 2. Coherencia

Artículo 63. *Mecanismo de coherencia.*

A fin de contribuir a la aplicación coherente del presente Reglamento en toda la Unión, las autoridades de control cooperarán entre sí y, en su caso, con la Comisión, en el marco del mecanismo de coherencia establecido en la presente sección.

Artículo 64. *Dictamen del Comité.*

1. El Comité emitirá un dictamen siempre que una autoridad de control competente proyecte adoptar alguna de las medidas enumeradas a continuación. A tal fin, la autoridad de control competente comunicará el proyecto de decisión al Comité, cuando la decisión:

a) tenga por objeto adoptar una lista de las operaciones de tratamiento supeditadas al requisito de la evaluación de impacto relativa a la protección de datos de conformidad con el artículo 35, apartado 4;

b) afecte a un asunto de conformidad con el artículo 40, apartado 7, cuyo objeto sea determinar si un proyecto de código de conducta o una modificación o ampliación de un código de conducta es conforme con el presente Reglamento;

c) tenga por objeto aprobar los requisitos para la acreditación de un organismo con arreglo al artículo 41, apartado 3, de un organismo de certificación conforme al artículo 43, apartado 3, o los criterios aplicables a la certificación a que se refiere el artículo 42, apartado 5;

d) tenga por objeto determinar las cláusulas tipo de protección de datos contempladas en el artículo 46, apartado 2, letra d), y el artículo 28, apartado 8;

e) tenga por objeto autorizar las cláusulas contractuales a que se refiere el artículo 46, apartado 3, letra a);

f) tenga por objeto la aprobación de normas corporativas vinculantes a tenor del artículo 47.

2. Cualquier autoridad de control, el presidente del Comité o la Comisión podrán solicitar que cualquier asunto de aplicación general o que surta efecto en más de un Estado miembro sea examinado por el Comité a efectos de dictamen, en particular cuando una autoridad de control competente incumpla las obligaciones relativas a la asistencia mutua con arreglo al artículo 61 o las operaciones conjuntas con arreglo al artículo 62.

3. En los casos a que se refieren los apartados 1 y 2, el Comité emitirá dictamen sobre el asunto que le haya sido presentado siempre que no haya emitido ya un dictamen sobre el mismo asunto. Dicho dictamen se adoptará en el plazo de ocho semanas por mayoría simple de los miembros del Comité. Dicho plazo podrá prorrogarse seis semanas más, teniendo en cuenta la complejidad del asunto. Por lo que respecta al proyecto de decisión a que se refiere el apartado 1 y distribuido a los miembros del Comité con arreglo al apartado 5, todo miembro que no haya presentado objeciones dentro de un plazo razonable indicado por el presidente se considerará conforme con el proyecto de decisión.

4. Las autoridades de control y la Comisión comunicarán sin dilación por vía electrónica al Comité, utilizando un formato normalizado, toda información útil, en particular, cuando proceda, un resumen de los hechos, el proyecto de decisión, los motivos por los que es necesaria tal medida, y las opiniones de otras autoridades de control interesadas.

5. La Presidencia del Comité informará sin dilación indebida por medios electrónicos:

a) a los miembros del Comité y a la Comisión de cualquier información pertinente que le haya sido comunicada, utilizando un formato normalizado. La secretaría del Comité facilitará, de ser necesario, traducciones de la información que sea pertinente, y

b) a la autoridad de control contemplada, en su caso, en los apartados 1 y 2 y a la Comisión del dictamen, y lo publicará.

6. La autoridad de control competente a que se refiere el apartado 1 no adoptará su proyecto de decisión a tenor del apartado 1 en el plazo mencionado en el apartado 3.

7. La autoridad de control competente a que se refiere el apartado 1 tendrá en cuenta en la mayor medida posible el dictamen del Comité y, en el plazo de dos semanas desde la recepción del dictamen, comunicará por medios electrónicos al presidente del Comité si va a mantener o modificar su proyecto de decisión y, si lo hubiera, el proyecto de decisión modificado, utilizando un formato normalizado.

8. Cuando la autoridad de control competente a que se refiere el apartado 1 informe al presidente del Comité, en el plazo mencionado en el apartado 7 del presente artículo, de que no prevé seguir el dictamen del Comité, en todo o en parte, alegando los motivos correspondientes, se aplicará el artículo 65, apartado 1.

Artículo 65. *Resolución de conflictos por el Comité.*

1. Con el fin de garantizar una aplicación correcta y coherente del presente Reglamento en casos concretos, el Comité adoptará una decisión vinculante en los siguientes casos:

a) cuando, en un caso mencionado en el artículo 60, apartado 4, una autoridad de control interesada haya manifestado una objeción pertinente y motivada a un proyecto de decisión de la autoridad de control principal y esta no haya seguido la objeción o haya rechazado dicha objeción por no ser pertinente o no estar motivada. La decisión vinculante afectará a todos los asuntos a que se refiera la objeción pertinente y motivada, en particular si hay infracción del presente Reglamento;

b) cuando haya puntos de vista enfrentados sobre cuál de las autoridades de control interesadas es competente para el establecimiento principal;

c) cuando una autoridad de control competente no solicite dictamen al Comité en los casos contemplados en el artículo 64, apartado 1, o no siga el dictamen del Comité emitido en virtud del artículo 64. En tal caso, cualquier autoridad de control interesada, o la Comisión, lo pondrá en conocimiento del Comité.

2. La decisión a que se refiere el apartado 1 se adoptará en el plazo de un mes a partir de la remisión del asunto, por mayoría de dos tercios de los miembros del Comité. Este plazo podrá prorrogarse un mes más, habida cuenta de la complejidad del asunto. La decisión que menciona el apartado 1 estará motivada y será dirigida a la autoridad de control principal y a todas las autoridades de control interesadas, y será vinculante para ellas.

3. Cuando el Comité no haya podido adoptar una decisión en los plazos mencionados en el apartado 2, adoptará su decisión en un plazo de dos semanas tras la expiración del segundo mes a que se refiere el apartado 2, por mayoría simple de sus miembros. En caso de empate, decidirá el voto del presidente.

4. Las autoridades de control interesadas no adoptarán decisión alguna sobre el asunto presentado al Comité en virtud del apartado 1 durante los plazos de tiempo a que se refieren los apartados 2 y 3.

5. El presidente del Comité notificará sin dilación indebida la decisión contemplada en el apartado 1 a las autoridades de control interesadas. También informará de ello a la Comisión. La decisión se publicará en el sitio web del Comité sin demora, una vez que la autoridad de control haya notificado la decisión definitiva a que se refiere el apartado 6.

6. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación adoptará su decisión definitiva sobre la base de la decisión contemplada en el apartado 1 del presente artículo, sin dilación indebida y a más tardar un mes tras la notificación de la decisión del Comité. La autoridad de control principal o, en su caso, la autoridad de control ante la que se presentó la reclamación informará al Comité de la fecha de notificación de su decisión definitiva al responsable o al encargado del

tratamiento y al interesado, respectivamente. La decisión definitiva de las autoridades de control interesadas será adoptada en los términos establecidos en el artículo 60, apartados 7, 8 y 9. La decisión definitiva hará referencia a la decisión contemplada en el apartado 1 del presente artículo y especificará que esta última decisión se publicará en el sitio web del Comité con arreglo al apartado 5 del presente artículo. La decisión definitiva llevará adjunta la decisión contemplada en el apartado 1 del presente artículo.

Artículo 66. *Procedimiento de urgencia.*

1. En circunstancias excepcionales, cuando una autoridad de control interesada considere que es urgente intervenir para proteger los derechos y las libertades de interesados, podrá, como excepción al mecanismo de coherencia contemplado en los artículos 63, 64 y 65, o al procedimiento mencionado en el artículo 60, adoptar inmediatamente medidas provisionales destinadas a producir efectos jurídicos en su propio territorio, con un periodo de validez determinado que no podrá ser superior a tres meses. La autoridad de control comunicará sin dilación dichas medidas, junto con los motivos de su adopción, a las demás autoridades de control interesadas, al Comité y a la Comisión.

2. Cuando una autoridad de control haya adoptado una medida de conformidad con el apartado 1, y considere que deben adoptarse urgentemente medidas definitivas, podrá solicitar con carácter urgente un dictamen o una decisión vinculante urgente del Comité, motivando dicha solicitud de dictamen o decisión.

3. Cualquier autoridad de control podrá solicitar, motivando su solicitud, y, en particular, la urgencia de la intervención, un dictamen urgente o una decisión vinculante urgente, según el caso, del Comité, cuando una autoridad de control competente no haya tomado una medida apropiada en una situación en la que sea urgente intervenir a fin de proteger los derechos y las libertades de los interesados.

4. No obstante lo dispuesto en el artículo 64, apartado 3, y en el artículo 65, apartado 2, los dictámenes urgentes o decisiones vinculantes urgentes contemplados en los apartados 2 y 3 del presente artículo se adoptarán en el plazo de dos semanas por mayoría simple de los miembros del Comité.

Artículo 67. *Intercambio de información.*

La Comisión podrá adoptar actos de ejecución de ámbito general para especificar las modalidades de intercambio de información por medios electrónicos entre las autoridades de control, y entre dichas autoridades y el Comité, en especial el formato normalizado contemplado en el artículo 64.

Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.

Sección 3. Comité europeo de protección de datos

Artículo 68. *Comité Europeo de Protección de Datos.*

1. Se crea el Comité Europeo de Protección de Datos («Comité»), como organismo de la Unión, que gozará de personalidad jurídica.

2. El Comité estará representado por su presidente.

3. El Comité estará compuesto por el director de una autoridad de control de cada Estado miembro y por el Supervisor Europeo de Protección de Datos o sus representantes respectivos.

4. Cuando en un Estado miembro estén encargados de controlar la aplicación de las disposiciones del presente Reglamento varias autoridades de control, se nombrará a un representante común de conformidad con el Derecho de ese Estado miembro.

5. La Comisión tendrá derecho a participar en las actividades y reuniones del Comité, sin derecho a voto. La Comisión designará un representante. El presidente del Comité comunicará a la Comisión las actividades del Comité.

6. En los casos a que se refiere el artículo 65, el Supervisor Europeo de Protección de Datos sólo tendrá derecho a voto en las decisiones relativas a los principios y normas

aplicables a las instituciones, órganos y organismos de la Unión que correspondan en cuanto al fondo a las contempladas en el presente Reglamento.

Artículo 69. *Independencia.*

1. El Comité actuará con total independencia en el desempeño de sus funciones o el ejercicio de sus competencias con arreglo a los artículos 70 y 71.

2. Sin perjuicio de las solicitudes de la Comisión contempladas en el artículo 70, apartados 1 y 2, el Comité no solicitará ni admitirá instrucciones de nadie en el desempeño de sus funciones o el ejercicio de sus competencias.

Artículo 70. *Funciones del Comité.*

1. El Comité garantizará la aplicación coherente del presente Reglamento. A tal efecto, el Comité, a iniciativa propia o, en su caso, a instancia de la Comisión, en particular:

a) supervisará y garantizará la correcta aplicación del presente Reglamento en los casos contemplados en los artículos 64 y 65, sin perjuicio de las funciones de las autoridades de control nacionales;

b) asesorará a la Comisión sobre toda cuestión relativa a la protección de datos personales en la Unión, en particular sobre cualquier propuesta de modificación del presente Reglamento;

c) asesorará a la Comisión sobre el formato y los procedimientos para intercambiar información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes;

d) emitirá directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales procedentes de servicios de comunicación a disposición pública a que se refiere el artículo 17, apartado 2;

e) examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento;

f) emitirá directrices, recomendaciones y buenas prácticas de conformidad con la letra e) del presente apartado a fin de especificar más los criterios y requisitos de las decisiones basadas en perfiles en virtud del artículo 22, apartado 2;

g) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de constatar las violaciones de la seguridad de los datos y determinar la dilación indebida a tenor del artículo 33, apartados 1 y 2, y con respecto a las circunstancias particulares en las que el responsable o el encargado del tratamiento debe notificar la violación de la seguridad de los datos personales;

h) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con respecto a las circunstancias en las que sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas a tenor del artículo 34, apartado 1;

i) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado con el fin de especificar en mayor medida los criterios y requisitos para las transferencias de datos personales basadas en normas corporativas vinculantes a las que se hayan adherido los responsables del tratamiento y en normas corporativas vinculantes a las que se hayan adherido los encargados del tratamiento y en requisitos adicionales necesarios para garantizar la protección de los datos personales de los interesados a que se refiere el artículo 47;

j) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de especificar en mayor medida los criterios y requisitos de las transferencias de datos personales sobre la base del artículo 49, apartado 1;

k) formulará directrices para las autoridades de control, relativas a la aplicación de las medidas a que se refiere el artículo 58, apartados 1, 2 y 3, y la fijación de multas administrativas de conformidad con el artículo 83;

l) examinará la aplicación práctica de las directrices, recomendaciones y buenas prácticas;

m) emitirá directrices, recomendaciones y buenas prácticas con arreglo a la letra e) del presente apartado a fin de establecer procedimientos comunes de información procedente de personas físicas sobre infracciones del presente Reglamento en virtud del artículo 54, apartado 2;

n) alentará la elaboración de códigos de conducta y el establecimiento de mecanismos de certificación de la protección de datos y de sellos y marcas de protección de datos de conformidad con los artículos 40 y 42;

o) aprobará los criterios de certificación en virtud del artículo 42, apartado 5, y llevará un registro público de los mecanismos de certificación y sellos y marcas de protección de datos en virtud del artículo 42, apartado 8, y de los responsables o los encargados del tratamiento certificados establecidos en terceros países en virtud del artículo 42, apartado 7;

p) aprobará los requisitos contemplados en el artículo 43, apartado 3, con miras a la acreditación de los organismos de certificación a los que se refiere el artículo 43;

q) facilitará a la Comisión un dictamen sobre los requisitos de certificación contemplados en el artículo 43, apartado 8;

r) facilitará a la Comisión un dictamen sobre los iconos a que se refiere el artículo 12, apartado 7;

s) facilitará a la Comisión un dictamen para evaluar la adecuación del nivel de protección en un tercer país u organización internacional, en particular para evaluar si un tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o una organización internacional, ya no garantizan un nivel de protección adecuado. A tal fin, la Comisión facilitará al Comité toda la documentación necesaria, incluida la correspondencia con el gobierno del tercer país, que se refiera a dicho tercer país, territorio o específico o a dicha organización internacional;

t) emitirá dictámenes sobre los proyectos de decisión de las autoridades de control en virtud del mecanismo de coherencia mencionado en el artículo 64, apartado 1, sobre los asuntos presentados en virtud del artículo 64, apartado 2, y sobre las decisiones vinculantes en virtud del artículo 65, incluidos los casos mencionados en el artículo 66;

u) promoverá la cooperación y los intercambios bilaterales y multilaterales efectivos de información y de buenas prácticas entre las autoridades de control;

v) promoverá programas de formación comunes y facilitará intercambios de personal entre las autoridades de control y, cuando proceda, con las autoridades de control de terceros países o con organizaciones internacionales;

w) promoverá el intercambio de conocimientos y documentación sobre legislación y prácticas en materia de protección de datos con las autoridades de control encargadas de la protección de datos a escala mundial;

x) emitirá dictámenes sobre los códigos de conducta elaborados a escala de la Unión de conformidad con el artículo 40, apartado 9, y

y) llevará un registro electrónico, de acceso público, de las decisiones adoptadas por las autoridades de control y los tribunales sobre los asuntos tratados en el marco del mecanismo de coherencia.

2. Cuando la Comisión solicite asesoramiento del Comité podrá señalar un plazo teniendo en cuenta la urgencia del asunto.

3. El Comité transmitirá sus dictámenes, directrices, recomendaciones y buenas prácticas a la Comisión y al Comité contemplado en el artículo 93, y los hará públicos.

4. Cuando proceda, el Comité consultará a las partes interesadas y les dará la oportunidad de presentar sus comentarios en un plazo razonable. Sin perjuicio de lo dispuesto en el artículo 76, el Comité publicará los resultados del procedimiento de consulta.

Artículo 71. *Informes.*

1. El Comité elaborará un informe anual en materia de protección de las personas físicas en lo que respecta al tratamiento en la Unión y, si procede, en terceros países y organizaciones internacionales. El informe se hará público y se transmitirá al Parlamento Europeo, al Consejo y a la Comisión.

2. El informe anual incluirá un examen de la aplicación práctica de las directrices, recomendaciones y buenas prácticas indicadas en el artículo 70, apartado 1, letra l), así como de las decisiones vinculantes indicadas en el artículo 65.

Artículo 72. *Procedimiento.*

1. El Comité tomará sus decisiones por mayoría simple de sus miembros, salvo que el presente Reglamento disponga otra cosa.
2. El Comité adoptará su reglamento interno por mayoría de dos tercios de sus miembros y organizará sus disposiciones de funcionamiento.

Artículo 73. *Presidencia.*

1. El Comité elegirá por mayoría simple de entre sus miembros un presidente y dos vicepresidentes.
2. El mandato del presidente y de los vicepresidentes será de cinco años de duración y podrá renovarse una vez.

Artículo 74. *Funciones del presidente.*

1. El presidente desempeñará las siguientes funciones:

a) convocar las reuniones del Comité y preparar su orden del día;
b) notificar las decisiones adoptadas por el Comité con arreglo al artículo 65 a la autoridad de control principal y a las autoridades de control interesadas;
c) garantizar el ejercicio puntual de las funciones del Comité, en particular en relación con el mecanismo de coherencia a que se refiere el artículo 63.

2. El Comité determinará la distribución de funciones entre el presidente y los vicepresidentes en su reglamento interno.

Artículo 75. *Secretaría.*

1. El Comité contará con una secretaría, de la que se hará cargo el Supervisor Europeo de Protección de Datos.
2. La secretaría ejercerá sus funciones siguiendo exclusivamente las instrucciones del presidente del Comité.
3. El personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento dependerá de un superior jerárquico distinto del personal que desempeñe las funciones conferidas al Supervisor Europeo de Protección de Datos.
4. El Comité, en consulta con el Supervisor Europeo de Protección de Datos, elaborará y publicará, si procede, un memorando de entendimiento para la puesta en práctica del presente artículo, que determinará los términos de su cooperación y que será aplicable al personal del Supervisor Europeo de Protección de Datos que participe en el desempeño de las funciones conferidas al Comité por el presente Reglamento.
5. La secretaría prestará apoyo analítico, administrativo y logístico al Comité.
6. La secretaría será responsable, en particular, de:

a) los asuntos corrientes del Comité;
b) la comunicación entre los miembros del Comité, su presidente y la Comisión;
c) la comunicación con otras instituciones y con el público;
d) la utilización de medios electrónicos para la comunicación interna y externa;
e) la traducción de la información pertinente;
f) la preparación y el seguimiento de las reuniones del Comité;
g) la preparación, redacción y publicación de dictámenes, decisiones relativas a solución de diferencias entre autoridades de control y otros textos adoptados por el Comité.

Artículo 76. *Confidencialidad.*

1. Los debates del Comité serán confidenciales cuando el mismo lo considere necesario, tal como establezca su reglamento interno.

2. El acceso a los documentos presentados a los miembros del Comité, los expertos y los representantes de terceras partes se regirá por el Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo [21].

[21] Reglamento (CE) n.º 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DO L 145 de 31.5.2001, p. 43).

CAPÍTULO VIII

Recursos, responsabilidad y sanciones

Artículo 77. *Derecho a presentar una reclamación ante una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, en particular en el Estado miembro en el que tenga su residencia habitual, lugar de trabajo o lugar de la supuesta infracción, si considera que el tratamiento de datos personales que le conciernen infringe el presente Reglamento.

2. La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78.

Artículo 78. *Derecho a la tutela judicial efectiva contra una autoridad de control.*

1. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna.

2. Sin perjuicio de cualquier otro recurso administrativo o extrajudicial, todo interesado tendrá derecho a la tutela judicial efectiva en caso de que la autoridad de control que sea competente en virtud de los artículos 55 y 56 no dé curso a una reclamación o no informe al interesado en el plazo de tres meses sobre el curso o el resultado de la reclamación presentada en virtud del artículo 77.

3. Las acciones contra una autoridad de control deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la autoridad de control.

4. Cuando se ejerciten acciones contra una decisión de una autoridad de control que haya sido precedida de un dictamen o una decisión del Comité en el marco del mecanismo de coherencia, la autoridad de control remitirá al tribunal dicho dictamen o decisión.

Artículo 79. *Derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento.*

1. Sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante una autoridad de control en virtud del artículo 77, todo interesado tendrá derecho a la tutela judicial efectiva cuando considere que sus derechos en virtud del presente Reglamento han sido vulnerados como consecuencia de un tratamiento de sus datos personales.

2. Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos.

Artículo 80. *Representación de los interesados.*

1. El interesado tendrá derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida con arreglo al Derecho de un Estado miembro, cuyos objetivos estatutarios sean de interés público y que actúe en el

ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77, 78 y 79, y el derecho a ser indemnizado mencionado en el artículo 82 si así lo establece el Derecho del Estado miembro.

2. Cualquier Estado miembro podrán disponer que cualquier entidad, organización o asociación mencionada en el apartado 1 del presente artículo tenga, con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos del interesado con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento.

Artículo 81. *Suspensión de los procedimientos.*

1. Cuando un tribunal competente de un Estado miembro tenga información de la pendencia ante un tribunal de otro Estado miembro de un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado, se pondrá en contacto con dicho tribunal de otro Estado miembro para confirmar la existencia de dicho procedimiento.

2. Cuando un procedimiento relativo a un mismo asunto en relación con el tratamiento por el mismo responsable o encargado esté pendiente ante un tribunal de otro Estado miembro, cualquier tribunal competente distinto de aquel ante el que se ejercitó la acción en primer lugar podrá suspender su procedimiento.

3. Cuando dicho procedimiento esté pendiente en primera instancia, cualquier tribunal distinto de aquel ante el que se ejercitó la acción en primer lugar podrá también, a instancia de una de las partes, inhibirse en caso de que el primer tribunal sea competente para su conocimiento y su acumulación sea conforme a Derecho.

Artículo 82. *Derecho a indemnización y responsabilidad.*

1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos.

2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable.

3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios.

4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado.

5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2.

6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2.

Artículo 83. *Condiciones generales para la imposición de multas administrativas.*

1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

3. Si un responsable o un encargado del tratamiento incumpliera de forma intencionada o negligente, para las mismas operaciones de tratamiento u operaciones vinculadas, diversas disposiciones del presente Reglamento, la cuantía total de la multa administrativa no será superior a la cuantía prevista para las infracciones más graves.

4. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones del organismo de supervisión a tenor del artículo 41, apartado 4.

5. Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1.

6. El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

7. Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

8. El ejercicio por una autoridad de control de sus poderes en virtud del presente artículo estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros, entre ellas la tutela judicial efectiva y el respeto de las garantías procesales.

9. Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias. Los Estados miembros de que se trate notificarán a la Comisión las disposiciones legislativas que adopten en virtud del presente apartado a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier ley de modificación o modificación posterior que les sea aplicable.

Artículo 84. *Sanciones.*

1. Los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias.

2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior que les sea aplicable.

CAPÍTULO IX

Disposiciones relativas a situaciones específicas de tratamiento

Artículo 85. *Tratamiento y libertad de expresión y de información.*

1. Los Estados miembros conciliarán por ley el derecho a la protección de los datos personales en virtud del presente Reglamento con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria.

2. Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información.

3. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 2 y, sin dilación, cualquier modificación posterior, legislativa u otra, de las mismas.

Artículo 86. *Tratamiento y acceso del público a documentos oficiales.*

Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento.

Artículo 87. *Tratamiento del número nacional de identificación.*

Los Estados miembros podrán determinar adicionalmente las condiciones específicas para el tratamiento de un número nacional de identificación o cualquier otro medio de identificación de carácter general. En ese caso, el número nacional de identificación o cualquier otro medio de identificación de carácter general se utilizará únicamente con las garantías adecuadas para los derechos y las libertades del interesado con arreglo al presente Reglamento.

Artículo 88. *Tratamiento en el ámbito laboral.*

1. Los Estados miembros podrán, a través de disposiciones legislativas o de convenios colectivos, establecer normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral, en particular a efectos de contratación de personal, ejecución del contrato laboral, incluido el cumplimiento de las obligaciones establecidas por la ley o por el convenio colectivo, gestión, planificación y organización del trabajo, igualdad y diversidad en el lugar de trabajo, salud y seguridad en el trabajo, protección de los bienes de empleadores o clientes, así como a efectos del ejercicio y disfrute, individual o colectivo, de los derechos y prestaciones relacionados con el empleo y a efectos de la extinción de la relación laboral.

2. Dichas normas incluirán medidas adecuadas y específicas para preservar la dignidad humana de los interesados así como sus intereses legítimos y sus derechos fundamentales, prestando especial atención a la transparencia del tratamiento, a la transferencia de los datos personales dentro de un grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta y a los sistemas de supervisión en el lugar de trabajo.

3. Cada Estado miembro notificará a la Comisión las disposiciones legales que adopte de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 89. *Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.*

1. El tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo.

2. Cuando se traten datos personales con fines de investigación científica o histórica o estadísticos el Derecho de la Unión o de los Estados miembros podrá establecer excepciones a los derechos contemplados en los artículos 15, 16, 18 y 21, sujetas a las condiciones y garantías indicadas en el apartado 1 del presente artículo, siempre y cuando sea probable que esos derechos imposibiliten u obstaculicen gravemente el logro de los fines científicos y cuando esas excepciones sean necesarias para alcanzar esos fines.

3. Cuando se traten datos personales con fines de archivo en interés público, el Derecho de le Unión o de los Estados miembros podrá prever excepciones a los derechos contemplados en los artículos 15, 16, 18, 19, 20 y 21, sujetas a las condiciones y garantías citadas en el apartado 1 del presente artículo, siempre que esos derechos puedan imposibilitar u obstaculizar gravemente el logro de los fines científicos y cuanto esas excepciones sean necesarias para alcanzar esos fines.

4. En caso de que el tratamiento a que hacen referencia los apartados 2 y 3 sirva también al mismo tiempo a otro fin, las excepciones solo serán aplicables al tratamiento para los fines mencionados en dichos apartados.

Artículo 90. *Obligaciones de secreto.*

1. Los Estados miembros podrán adoptar normas específicas para fijar los poderes de las autoridades de control establecidos en el artículo 58, apartado 1, letras e) y f), en relación con los responsables o encargados sujetos, con arreglo al Derecho de la Unión o de los Estados miembros o a las normas establecidas por los organismos nacionales competentes, a una obligación de secreto profesional o a otras obligaciones de secreto equivalentes, cuando sea necesario y proporcionado para conciliar el derecho a la protección de los datos personales con la obligación de secreto. Esas normas solo se aplicarán a los datos personales que el responsable o el encargado del tratamiento hayan recibido como resultado o con ocasión de una actividad cubierta por la citada obligación de secreto.

2. Cada Estado miembro notificará a la Comisión las normas adoptadas de conformidad con el apartado 1 a más tardar el 25 de mayo de 2018 y, sin dilación, cualquier modificación posterior de las mismas.

Artículo 91. *Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas.*

1. Cuando en un Estado miembro iglesias, asociaciones o comunidades religiosas apliquen, en el momento de la entrada en vigor del presente Reglamento, un conjunto de normas relativas a la protección de las personas físicas en lo que respecta al tratamiento, tales normas podrán seguir aplicándose, siempre que sean conformes con el presente Reglamento.

2. Las iglesias y las asociaciones religiosas que apliquen normas generales de conformidad con el apartado 1 del presente artículo estarán sujetas al control de una autoridad de control independiente, que podrá ser específica, siempre que cumpla las condiciones establecidas en el capítulo VI del presente Reglamento.

CAPÍTULO X

Actos delegados y actos de ejecución

Artículo 92. *Ejercicio de la delegación.*

1. Los poderes para adoptar actos delegados otorgados a la Comisión estarán sujetos a las condiciones establecidas en el presente artículo.

2. La delegación de poderes indicada en el artículo 12, apartado 8, y en el artículo 43, apartado 8, se otorgarán a la Comisión por tiempo indefinido a partir del 24 de mayo de 2016.

3. La delegación de poderes mencionada en el artículo 12, apartado 8, y el artículo 43, apartado 8, podrá ser revocada en cualquier momento por el Parlamento Europeo o por el Consejo. La decisión de revocación pondrá término a la delegación de los poderes que en ella se especifiquen. La decisión surtirá efecto al día siguiente de su publicación en el Diario Oficial de la Unión Europea o en una fecha posterior indicada en la misma. No afectará a la validez de los actos delegados que ya estén en vigor.

4. Tan pronto como la Comisión adopte un acto delegado lo notificará simultáneamente al Parlamento Europeo y al Consejo.

5. Los actos delegados adoptados en virtud del artículo 12, apartado 8, y el artículo 43, apartado 8, entrarán en vigor únicamente si, en un plazo de tres meses desde su notificación

al Parlamento Europeo y al Consejo, ni el Parlamento Europeo ni el Consejo formulan objeciones o si, antes del vencimiento de dicho plazo, tanto el uno como el otro informan a la Comisión de que no las formularán. El plazo se ampliará en tres meses a iniciativa del Parlamento Europeo o del Consejo.

Artículo 93. *Procedimiento de comité.*

1. La Comisión estará asistida por un comité. Dicho comité será un comité en el sentido del Reglamento (UE) n.º 182/2011.
2. Cuando se haga referencia al presente apartado, se aplicará el artículo 5 del Reglamento (UE) n.º 182/2011.
3. Cuando se haga referencia al presente apartado, se aplicará el artículo 8 del Reglamento (UE) n.º 182/2011, en relación con su artículo 5.

CAPÍTULO XI

Disposiciones finales

Artículo 94. *Derogación de la Directiva 95/46/CE.*

1. Queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018.
2. Toda referencia a la Directiva derogada se entenderá hecha al presente Reglamento. Toda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento.

Artículo 95. *Relación con la Directiva 2002/58/CE.*

El presente Reglamento no impondrá obligaciones adicionales a las personas físicas o jurídicas en materia de tratamiento en el marco de la prestación de servicios públicos de comunicaciones electrónicas en redes públicas de comunicación de la Unión en ámbitos en los que estén sujetas a obligaciones específicas con el mismo objetivo establecidas en la Directiva 2002/58/CE.

Artículo 96. *Relación con acuerdos celebrados anteriormente.*

Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 24 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable antes de dicha fecha, seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Artículo 97. *Informes de la Comisión.*

1. A más tardar el 25 de mayo de 2020 y posteriormente cada cuatro años, la Comisión presentará al Parlamento Europeo y al Consejo un informe sobre la evaluación y revisión del presente Reglamento. Los informes se harán públicos.
2. En el marco de las evaluaciones y revisiones a que se refiere el apartado 1, la Comisión examinará en particular la aplicación y el funcionamiento de:

a) el capítulo V sobre la transferencia de datos personales a países terceros u organizaciones internacionales, particularmente respecto de las decisiones adoptadas en virtud del artículo 45, apartado 3, del presente Reglamento, y de las adoptadas sobre la base del artículo 25, apartado 6, de la Directiva 95/46/CE;
b) el capítulo VII sobre cooperación y coherencia.

3. A los efectos del apartado 1, la Comisión podrá solicitar información a los Estados miembros y a las autoridades de control.
4. Al llevar a cabo las evaluaciones y revisiones indicadas en los apartados 1 y 2, la Comisión tendrá en cuenta las posiciones y conclusiones del Parlamento Europeo, el Consejo y los demás órganos o fuentes pertinentes.

5. La Comisión presentará, en caso necesario, las propuestas oportunas para modificar el presente Reglamento, en particular teniendo en cuenta la evolución de las tecnologías de la información y a la vista de los progresos en la sociedad de la información.

Artículo 98. *Revisión de otros actos jurídicos de la Unión en materia de protección de datos.*

La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos.

Artículo 99. *Entrada en vigor y aplicación.*

1. El presente Reglamento entrará en vigor a los veinte días de su publicación en el Diario Oficial de la Unión Europea.
2. Será aplicable a partir del 25 de mayo de 2018.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

§ 65

Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia

Jefatura del Estado
«BOE» núm. 160, de 6 de julio de 2011
Última modificación: 19 de septiembre de 2020
Referencia: BOE-A-2011-11605

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

Todas las personas tienen derecho a obtener la tutela efectiva de sus derechos ante los tribunales. Así se reconoce en nuestro ordenamiento jurídico en el artículo 24.1 de la Constitución y en el artículo 14.1 del Pacto Internacional de Derechos Civiles y Políticos. Para salvaguardar dichos derechos de los ciudadanos es necesaria la modernización de la Administración de Justicia, campo esencial para consolidar el Estado de Derecho y mejorar la calidad de nuestra democracia. En este contexto de modernización, uno de los elementos de mayor relevancia es, precisamente, la incorporación en las oficinas judiciales de las nuevas tecnologías. Su uso generalizado y obligatorio contribuirá a mejorar la gestión en las oficinas judiciales, actualizando su funcionamiento e incrementando los niveles de eficiencia. Las nuevas tecnologías permiten igualmente abaratar los costes del servicio público de justicia, pero también suponen una mejora de la confianza en el sistema, lo que se traduce en mayor seguridad. Ello incide de manera directa e indirecta en el sistema económico, pues los cambios generan nuevas perspectivas en las relaciones económicas, acrecentando la seguridad y la fluidez de las mismas.

La presente Ley regula el uso de las nuevas tecnologías en la Administración de Justicia. Los principales objetivos de esta norma, son: primero, actualizar el contenido del derecho fundamental a un proceso público sin dilaciones indebidas, gracias a la agilización que permite el uso de las tecnologías en las comunicaciones; segundo, generalizar el uso de las nuevas tecnologías para los profesionales de la justicia; tercero, definir en una norma con rango de ley el conjunto de requisitos mínimos de interconexión, interoperabilidad y seguridad necesarios en el desarrollo de los diferentes aplicativos utilizados por los actores

del mundo judicial, a fin de garantizar la seguridad en la transmisión de los datos y cuantas otras exigencias se contengan en las leyes procesales.

II

En nuestro ordenamiento jurídico existen ya distintos antecedentes que hacían necesaria la aprobación de esta norma.

Así, por un lado, la Ley Orgánica 16/1994, de 8 de noviembre, por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, introdujo, por vez primera en nuestro ordenamiento jurídico, la posibilidad de utilizar medios técnicos, electrónicos e informáticos para el desarrollo de la actividad y el ejercicio de las funciones de juzgados y tribunales. La reforma realizada incluía la posibilidad de dotar a los nuevos documentos o comunicaciones de la validez y eficacia de los originales, siempre que se garantizase la autenticidad, la integridad y el cumplimiento de los requisitos previstos en las leyes procesales.

A partir de esta reforma se han llevado a cabo numerosas modificaciones en distintas normas a fin de hacer efectiva esta previsión. Debe advertirse, eso sí, que estas modificaciones se han producido obedeciendo a necesidades concretas y puntuales detectadas casi siempre en las distintas leyes procesales. También se han aprobado normas relativas a la regulación de aplicaciones y sistemas informáticos utilizados en la Administración de Justicia, así como el establecimiento de registros y sistemas de información y apoyo a la actividad judicial.

El Pleno del Congreso de los Diputados aprobó el día 22 de abril de 2002 una Proposición no de Ley sobre la Carta de Derechos de los Ciudadanos ante la Justicia. Esta Carta señala en su preámbulo que, en los umbrales del siglo XXI, la sociedad española demandaba con urgencia una justicia más abierta que fuese capaz de dar respuesta a los ciudadanos con mayor agilidad, calidad y eficacia, incorporando para ello métodos de organización e instrumentos procesales más modernos y avanzados. Bajo el título «Una Justicia moderna y abierta a los ciudadanos», la primera parte de la Carta recoge los principios que deben inspirar la consecución de dicho objetivo: una justicia transparente y comprensible. El apartado 21, ahondando en la necesidad de que la justicia sea tecnológicamente avanzada, reconoce el derecho «a comunicarse con la Administración de Justicia a través del correo electrónico, videoconferencia y otros medios telemáticos con arreglo a lo dispuesto en las leyes procesales».

Más tarde, la Ley 15/2003, de 26 de mayo, reguladora del régimen retributivo de las carreras judicial y fiscal, consagra el objetivo general de transparencia proclamado en la Carta de Derechos de los Ciudadanos ante la Justicia, creando un instrumento técnico llamado Plan de Transparencia Judicial. Este Plan fue aprobado por Acuerdo de Consejo de Ministros de 21 de octubre de 2005. En él se identifica como instrumento imprescindible para lograr el objetivo de la transparencia la plena utilización de las tecnologías de la información y la comunicación en la Administración de Justicia. Para que este uso sea realidad es necesario unificar o hacer compatibles las distintas aplicaciones informáticas que se utilizan en las oficinas judiciales, así como crear páginas de información en las Administraciones con competencias en materia de justicia. También se declara la necesidad de establecer sistemas adecuados de interconexión y sistemas de intercambio seguro de documentos en los procesos judiciales, así como garantizar la disponibilidad de los sistemas de comunicaciones entre las distintas sedes judiciales electrónicas.

En otro orden de cosas, en 2007 se aprueba la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Esta norma supone el reconocimiento definitivo del derecho de los ciudadanos a comunicarse electrónicamente con las Administraciones públicas. Esta Ley establece el régimen jurídico de la administración electrónica y la gestión electrónica de los procedimientos administrativos y sienta las bases sobre las que debe articularse la cooperación entre las distintas Administraciones para impulsar la administración electrónica.

Por último, en el plano internacional, la Unión Europea ha desarrollado el Plan de Acción E-Justicia. Este Plan de Acción busca la mejora de la eficacia de los sistemas judiciales mediante la aplicación de las tecnologías de información y comunicación en la gestión administrativa de los procesos judiciales. El Plan busca también la cooperación entre las autoridades judiciales y, lo que es más importante, el acceso de los ciudadanos a la justicia.

Para ello, el Plan propone la adopción de medidas coordinadas a nivel nacional y europeo. Su aplicación implicará probablemente modificaciones y adaptaciones en la legislación procesal, así como la creación de un marco regulador de la utilización de las nuevas tecnologías en la Administración de Justicia española, que es el objetivo al que responde esta norma.

III

La Administración de Justicia presenta características que la diferencian de las restantes Administraciones públicas. En primer lugar, por la propia naturaleza de la función que la Administración judicial tiene atribuida, ya que se trata de un poder del Estado distinto del poder ejecutivo, en el que se encuadran las Administraciones públicas que, además, debe satisfacer un derecho fundamental que a su vez es clave para sostener el Estado de Derecho. En segundo lugar, la relación de los ciudadanos con los órganos judiciales se establece casi siempre a través de profesionales, cosa que no suele suceder en el caso de las Administraciones públicas.

Dadas estas características, se ha considerado que la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, no es plenamente aplicable a la Administración de Justicia y es necesaria una regulación específica. Ello no quiere decir, no obstante, que no se hayan adoptado idénticos principios y valores en muchos aspectos.

Así, se ha tenido en cuenta la diferencia entre el procedimiento administrativo y las normas procesales. La presente Ley regula únicamente los aspectos necesarios para dar cumplimiento a la legislación procesal en lo relativo al uso de las nuevas tecnologías. Así, por ejemplo, no se ha buscado establecer plazos o términos distintos de los señalados en las leyes de enjuiciamiento, sino que la norma se limita a establecer los criterios que deben ser considerados para efectuar el cómputo de los mismos si los actos procesales que determinan su comienzo o fin se efectúan a través de medios electrónicos.

También tiene una gran importancia la cooperación entre Administraciones en materia de administración electrónica. Para ello se establecen marcos estables y vinculantes de colaboración, cooperación y coordinación. En este capítulo cobra especial importancia la consolidación como norma legal de algunas de las previsiones contenidas en el Convenio de Colaboración entre el Ministerio de Justicia, el Consejo General del Poder Judicial y la Fiscalía General del Estado para el establecimiento del Esquema judicial de interoperabilidad y seguridad en el ámbito de la Administración de Justicia (EJIS). Asimismo, la Ley crea el Comité técnico estatal de la Administración judicial electrónica, que ostentará competencias en orden a la interoperabilidad de las distintas aplicaciones que se utilizan en la Administración de Justicia, sin perjuicio de las previstas para el Consejo General del Poder Judicial.

IV

La Ley consta de cincuenta y seis artículos agrupados en cinco títulos, doce disposiciones adicionales, dos disposiciones transitorias y cuatro disposiciones finales.

En el Título I se define el objeto de la Ley y su ámbito de aplicación.

El Título II se dedica a regular el uso de medios electrónicos en la Administración de Justicia y se estructura en tres capítulos. El primero de ellos recoge los derechos de los ciudadanos en sus relaciones con dicha Administración, reconociendo la libertad de elección a la hora de establecer tales relaciones y garantizando que la Administración le facilitará los medios necesarios para relacionarse electrónicamente, aún cuando el ciudadano no disponga de los mismos.

El Capítulo II recoge los derechos y deberes de los profesionales del ámbito de la justicia en sus relaciones con la misma por medios electrónicos. Abogados, procuradores, graduados sociales y demás profesionales que actúan en el ámbito de la justicia, además de tener reconocidos los derechos que le son necesarios para el ejercicio de su profesión, utilizarán los medios electrónicos para la presentación de sus escritos y documentos. Esta actividad permitirá la tramitación íntegramente electrónica de los procedimientos judiciales.

El tercer y último Capítulo de este Título recoge la obligación de todos los integrantes de los órganos y oficinas judiciales, así como de las fiscalías, de utilizar exclusivamente los

programas y aplicaciones informáticas puestas a su disposición por las Administraciones competentes.

El Título III aborda el régimen jurídico de la Administración judicial electrónica. En su Capítulo I se define lo que son las sedes judiciales electrónicas y se establece el contenido mínimo de las mismas. A través de dichas sedes se realizarán las actuaciones que lleven a cabo ciudadanos y profesionales con la Administración de Justicia. Se diferencia entre la titularidad de la sede, que viene atribuida a la Administración competente para dotar de medios materiales a los juzgados y tribunales, y el responsable de los contenidos de la misma, que será el órgano que origine la información que se incluya en la sede. Por lo tanto, el titular de una sede será únicamente uno y los responsables tantos como órganos hayan incluido contenidos en la misma. Especial atención merece la posibilidad de crear una o varias sedes electrónicas derivadas o subsedes. Por otro lado, se dispone la creación de un punto de acceso general de la Administración de Justicia, a través del cual se podrá acceder a todas las sedes y subsedes del territorio nacional, con independencia de la posibilidad de acceso directo a las mismas.

El Capítulo II se dedica a las formas de identificación y autenticación, tanto de ciudadanos y profesionales como de la propia Administración de Justicia. Respecto a los primeros, se contempla la posibilidad de uso de diversos sistemas de firma electrónica además del incorporado al Documento Nacional de Identidad. En cuanto a los órganos y oficinas judiciales, se establece la obligatoriedad de que la Administración competente facilite a los mismos los sistemas de firma electrónica consistentes en sello electrónico y código seguro de verificación. Asimismo, en este capítulo se regula el uso de la firma electrónica por parte de todo el personal al servicio de la Administración de Justicia. Por último, se establecen las condiciones para hacer posible la interoperabilidad y autenticación por medio de certificados electrónicos e intercambio electrónico de datos en entornos cerrados de comunicación.

El Título IV fija las condiciones para hacer posible la íntegra tramitación electrónica de los procedimientos judiciales. Dedica el Capítulo II a definir y regular el expediente judicial electrónico, heredero digital de los «autos» que tradicionalmente han constituido el decorado de nuestros juzgados y tribunales. Cuestiones tales como el foliado o la tradicional remisión de los autos, adquieren una dimensión totalmente diferente al amparo de las nuevas tecnologías. Se dispone igualmente qué documentos tienen la consideración de documentos judiciales electrónicos y se aborda una regulación de las copias electrónicas en función del formato del original. Por último, en este capítulo se dedica un artículo a establecer las condiciones en que se deben archivar los documentos judiciales electrónicos.

El Capítulo III de este Título trata del registro de escritos, de las comunicaciones y notificaciones electrónicas. Se establece el principio de que cada oficina judicial con funciones de registro y reparto tendrá asignada una sede electrónica derivada o subsede, de tal forma que cualquier escrito, oficio o comunicación dirigida a un órgano u oficina judicial a los que preste servicio de registro y reparto, deberá tener su entrada a través de dicha subsede electrónica. Se regula el régimen de funcionamiento de dicho registro, así como el cómputo de plazos. Se regula igualmente la forma en que deben comunicarse los ciudadanos y profesionales por medios electrónicos con la Administración de Justicia, así como las condiciones y requisitos que deben cumplir los sistemas que implanten las distintas Administraciones con competencias en las oficinas judiciales para la práctica de actos de comunicación por medios electrónicos.

El Capítulo IV contiene las previsiones relativas a la tramitación electrónica de los procedimientos judiciales. En cuanto al inicio del procedimiento, se establece la obligatoriedad de que el mismo lo sea siempre por medios electrónicos, distinguiendo los casos en que los ciudadanos lo inicien personalmente sin intervención de profesionales, en cuyo caso tendrán a su disposición los medios necesarios para poder hacerlo en dicha forma, de los casos en que comparezcan asistidos por profesionales, en los que serán estos los que tengan la obligación en todo caso de efectuar la presentación del escrito o demanda iniciadora del procedimiento en forma telemática.

Se establecen asimismo las características básicas que deben tener las aplicaciones y sistemas de información utilizados para la gestión por medios electrónicos de los procedimientos judiciales, en orden a garantizar aspectos esenciales de la tramitación

electrónica y la forma en que deben incorporarse a dichos procedimientos los escritos, documentos y otros medios o instrumentos que deban tener acceso a ellos.

Se prevé la forma en que las partes pueden utilizar medios electrónicos para ejercer el derecho reconocido en las leyes procesales a acceder a la información sobre el estado de tramitación de los procedimientos.

El Título V de la Ley aborda los aspectos básicos sobre los que debe asentarse la necesaria cooperación y colegiación de esfuerzos entre las Administraciones con competencias en materia de justicia. Se constituye el Comité técnico estatal de la Administración judicial electrónica con importantes competencias en orden a favorecer la compatibilidad y a asegurar la interoperabilidad de los sistemas y aplicaciones empleados en la Administración de Justicia, así como para asegurar la cooperación entre las distintas Administraciones.

Se define el contenido del Esquema judicial de interoperabilidad y seguridad, al considerarse dichas cualidades como esenciales para un eficaz y eficiente funcionamiento del sistema, estableciéndose que deberá tenerse presente y acomodarse al mismo todos los servicios, sistemas y aplicaciones utilizados en la Administración de Justicia a lo largo de su ciclo de vida.

Se establecen los principios generales a los que deberán responder tanto la interoperabilidad entre las distintas aplicaciones como la seguridad de la información contenida en ellas.

Como concreción del principio de cooperación al que obedece la presente Ley, se dispone la posibilidad de la reutilización de sistemas, infraestructuras y aplicaciones de las Administraciones con competencias en materia de justicia.

Por último, en las disposiciones adicionales se establecen los plazos a los que se deben ajustar las distintas Administraciones con competencias en materia de justicia para el íntegro establecimiento en las oficinas judiciales y fiscalías de los medios e instrumentos necesarios para la efectiva implantación de las tecnologías de la información y comunicación.

TÍTULO I

Del ámbito de aplicación y los principios generales

Artículo 1. *Objeto.*

1. La presente Ley regula la utilización de las tecnologías de la información por parte de los ciudadanos y profesionales en sus relaciones con la Administración de Justicia y en las relaciones de la Administración de Justicia con el resto de Administraciones y organismos públicos, en los términos recogidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

2. En la Administración de Justicia se utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando el acceso, la autenticidad, confidencialidad, integridad, disponibilidad, trazabilidad, conservación e interoperabilidad de los datos, informaciones y servicios que gestione en el ejercicio de sus funciones.

Artículo 2. *Ámbito de aplicación.*

La presente Ley será de aplicación a la Administración de Justicia, a los ciudadanos en sus relaciones con ella y a los profesionales que actúen en su ámbito, así como a las relaciones entre aquélla y el resto de Administraciones y organismos públicos.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley, los términos relacionados en el anexo tendrán el significado que resulta de las definiciones contenidas en el mismo.

TÍTULO II

Uso de los medios electrónicos en la Administración de Justicia

CAPÍTULO I

Derechos de los ciudadanos en sus relaciones con la Administración de Justicia por medios electrónicos

Artículo 4. *Derechos de los ciudadanos.*

1. Los ciudadanos tienen derecho a relacionarse con la Administración de Justicia utilizando medios electrónicos para el ejercicio de los derechos previstos en los Capítulos I y VII del Título III del Libro III de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la forma y con las limitaciones que en los mismos se establecen.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad judicial, y en los términos previstos en la presente Ley, los siguientes derechos:

a) A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con la Administración de Justicia.

b) A la igualdad en el acceso electrónico a los servicios de la Administración de Justicia.

c) A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean parte procesal legítima, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

d) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de parte o acrediten interés legítimo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

e) A la conservación en formato electrónico por la Administración de Justicia de los documentos electrónicos que formen parte de un expediente conforme a la normativa vigente en materia de archivos judiciales.

f) A utilizar los sistemas de identificación y firma establecidos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

g) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

h) A la calidad de los servicios públicos prestados por medios electrónicos.

i) A elegir las aplicaciones o sistemas para relacionarse con la Administración de Justicia siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos y, en todo caso, siempre que sean compatibles con los que dispongan los juzgados y tribunales y se respeten las garantías y requisitos previstos en el procedimiento que se trate.

Artículo 5. *Prestación de servicios y disposición de medios e instrumentos electrónicos.*

1. Las Administraciones con competencia en materia de justicia habilitarán diferentes canales o medios para la prestación de los servicios electrónicos, asegurando en todo caso el acceso a los mismos a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos, en la forma que estimen adecuada.

2. Las Administraciones competentes en materia de justicia asegurarán el acceso de todos los ciudadanos a los servicios electrónicos proporcionados en su ámbito a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:

a) Las oficinas de información y atención al público, en los procedimientos en los que los ciudadanos comparezcan y actúen sin asistencia letrada y sin representación procesal, pondrán a su disposición de forma libre y gratuita los medios e instrumentos precisos para

ejercer los derechos reconocidos en el artículo 4 de esta Ley, debiendo contar con asistencia y orientación sobre su utilización, bien a cargo del personal de las oficinas en que se ubiquen o bien por sistemas incorporados al propio medio o instrumento.

b) Puntos de acceso electrónico, consistentes en sedes judiciales electrónicas creadas y gestionadas por las distintas Administraciones competentes en materia de justicia y disponibles para los ciudadanos a través de redes de comunicación, para sus relaciones con la Administración de Justicia.

c) Las Administraciones con competencias en materia de justicia publicarán la relación de todos los puntos de acceso electrónico.

d) Servicios de atención telefónica con los criterios de seguridad y las posibilidades técnicas existentes, que faciliten a los ciudadanos las relaciones con la Administración de Justicia en lo que se refiere a los servicios electrónicos mencionados en los apartados anteriores.

e) Puntos de información electrónicos, ubicados en los edificios judiciales.

CAPÍTULO II

Derechos y deberes de los profesionales de la justicia en sus relaciones con la Administración de Justicia por medios electrónicos

Artículo 6. *Derechos y deberes de los profesionales del ámbito de la justicia.*

1. Los profesionales de la justicia tienen el derecho a relacionarse con la misma a través de medios electrónicos.

2. Además, los profesionales tienen, en relación con la utilización de los medios electrónicos en la actividad judicial y en los términos previstos en la presente Ley, los siguientes derechos:

a) A acceder y conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean representantes procesales de la parte personada, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

b) A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que sean representantes procesales de la parte personada o acrediten interés legítimo, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

c) A la conservación en formato electrónico por la Administración de Justicia de los documentos electrónicos que formen parte de un expediente según la normativa vigente en materia de archivos judiciales.

d) A utilizar los sistemas de identificación y firma establecidos en los artículos 9 y 10 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, siempre que dicho sistema le identifique de forma unívoca como profesional para cualquier trámite electrónico con la Administración en los términos establecidos por las leyes procesales.

A tal efecto, el Consejo General o el superior correspondiente deberá poner a disposición de las oficinas judiciales los protocolos y sistemas de interconexión que permitan el acceso necesario por medios electrónicos al registro de profesionales colegiados ejercientes previsto en el artículo 10 de la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, garantizando que en él consten sus datos profesionales, tales como número de colegiado, domicilio profesional, número de teléfono y dirección de correo electrónico.

e) A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

3. Los profesionales de la justicia, en los términos previstos en la presente Ley, tienen el deber de utilizar los medios electrónicos, las aplicaciones o los sistemas establecidos por las

Administraciones competentes en materia de justicia, respetando en todo caso las garantías y requisitos previstos en el procedimiento que se trate.

Artículo 7. *Prestación de servicios y disposición de medios e instrumentos electrónicos.*

Las Administraciones competentes en materia de justicia asegurarán el acceso de los profesionales a los servicios electrónicos proporcionados en su ámbito a través de puntos de acceso electrónico, consistentes en sedes judiciales electrónicas creadas y gestionadas por aquéllas y disponibles para los profesionales a través de redes de comunicación, para sus relaciones con la Administración de Justicia, en los términos previstos en la presente Ley.

CAPÍTULO III

Utilización obligatoria de los medios electrónicos en la tramitación de los procedimientos electrónicos judiciales

Artículo 8. *Uso obligatorio de medios e instrumentos electrónicos.*

Los sistemas informáticos puestos al servicio de la Administración de Justicia serán de uso obligatorio en el desarrollo de la actividad de los órganos y oficinas judiciales y de las fiscalías por parte de todos los integrantes de las mismas, conforme a los criterios e instrucciones de uso que dicten, en el ámbito de sus competencias, el Consejo General del Poder Judicial, la Fiscalía General del Estado y las Administraciones competentes, así como a los protocolos de actuación aprobados por los Secretarios de Gobierno.

Las Administraciones competentes proporcionarán los medios seguros para que estos sistemas sean plenamente accesibles y operativos sin necesidad de que los usuarios se encuentren físicamente en las sedes de sus respectivos órganos, oficinas o fiscalías.

TÍTULO III

Régimen jurídico de la Administración judicial electrónica

CAPÍTULO I

De la sede judicial electrónica

Artículo 9. *Sede judicial electrónica.*

1. La sede judicial electrónica es aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a cada una de las Administraciones competentes en materia de justicia.

2. Las sedes judiciales electrónicas se crearán mediante disposición publicada en el «Boletín Oficial del Estado» o el «Boletín Oficial de la Comunidad Autónoma» correspondiente, y tendrán, al menos, los siguientes contenidos:

a) Identificación de la dirección electrónica de referencia de la sede que incluya el nombre del dominio que le otorgue la Administración competente.

b) Identificación de su titular, así como del órgano u órganos administrativos encargados de la gestión y de los servicios puestos a disposición de los ciudadanos y profesionales en la misma.

c) Identificación de los canales de acceso a los servicios disponibles en la sede, con expresión, en su caso, de los teléfonos y oficinas a través de los cuales también puede accederse a los mismos.

d) Cauces disponibles para la formulación de sugerencias y quejas con respecto al servicio que presta la sede.

3. El establecimiento de una sede judicial electrónica conlleva la responsabilidad del titular de garantizar la integridad y actualización de la información facilitada, así como el acceso a los servicios previstos en la misma.

4. Las Administraciones competentes en materia de justicia determinarán las condiciones e instrumentos de creación de las sedes judiciales electrónicas, con sujeción a los principios de publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.

5. La publicación en las sedes judiciales electrónicas de informaciones, servicios y transacciones respetará los estándares abiertos y, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.

Artículo 10. *Características de las sedes judiciales electrónicas y sus clases.*

1. Se realizarán a través de sedes judiciales electrónicas todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración de Justicia o de los ciudadanos y profesionales por medios electrónicos.

2. Las sedes judiciales electrónicas dispondrán de sistemas que permitan el establecimiento de comunicaciones seguras siempre que sean necesarias.

3. Se podrán crear una o varias sedes judiciales electrónicas derivadas de una sede judicial electrónica. Las sedes judiciales electrónicas derivadas, o subsedes, deberán resultar accesibles desde la dirección electrónica de la sede principal, sin perjuicio de que sea posible el acceso electrónico directo.

4. La Administración competente creará una sede judicial electrónica derivada para cada uno de los servicios de recepción de escritos, registro y reparto de asuntos existentes, en función de su organización y cuyos contenidos serán gestionados por el propio servicio. En el caso de que exista un único servicio de recepción de escritos, registro y reparto, la sede judicial electrónica asumirá las funciones de las subsedes.

5. Igualmente la Administración competente creará una sede judicial electrónica derivada en cada una de las oficinas fiscales que tengan servicio de registro y reparto.

6. Las sedes judiciales electrónicas derivadas se crearán por disposición del órgano administrativo que tenga atribuida esta competencia y deberán cumplir los mismos requisitos de publicidad que las sedes judiciales electrónicas principales. Cuando los servicios de recepción de escritos, registro y reparto de asuntos no sean creados con una sede o subsede judicial electrónica, deberán recibir la misma publicidad que éstas.

Artículo 11. *Contenido y servicios de las sedes judiciales electrónicas.*

1. Toda sede judicial electrónica dispondrá, al menos, de los siguientes contenidos:

a) Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión, de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

b) Información necesaria para su correcta utilización, incluyendo el mapa de la sede judicial electrónica o información equivalente, con especificación de la estructura de navegación y las distintas secciones disponibles.

c) Sistema de verificación de los certificados de la sede, que estará accesible de forma directa y gratuita.

d) Relación de sistemas de firma electrónica que, conforme a lo previsto en esta Ley, sean admitidos o utilizados en la sede.

e) Normas de creación del registro o registros electrónicos accesibles desde la sede.

f) Información relacionada con la protección de datos de carácter personal, incluyendo un enlace con la sede electrónica de la Agencia Española de Protección de Datos y las de las Agencias Autonómicas de Protección de Datos.

2. Las sedes judiciales electrónicas dispondrán, al menos, de los siguientes servicios a disposición de los ciudadanos y profesionales:

a) La relación de los servicios disponibles en la sede judicial electrónica.

b) La carta de servicios y la carta de servicios electrónicos.

c) La relación de los medios electrónicos que los ciudadanos y profesionales pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con la Administración de Justicia.

d) Un enlace para la formulación de sugerencias y quejas ante los órganos correspondientes.

e) Acceso, en los términos legalmente establecidos, al estado de tramitación del expediente.

f) Un enlace al Tablón Edictal Judicial único, como medio de publicación y consulta de las resoluciones y comunicaciones que por disposición legal deban fijarse en el tablón de anuncios o edictos.

g) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

h) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

i) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.

j) La Carta de Derechos de los Ciudadanos ante la Justicia.

3. No será necesario recoger en las subsedes la información y los servicios a que se refieren los apartados anteriores cuando ya figuren en la sede de la que aquéllas derivan.

4. La sede judicial electrónica garantizará el régimen de cooficialidad lingüística vigente en su territorio.

Artículo 12. *Reglas especiales de responsabilidad.*

1. El órgano que origine la información que se deba incluir en la sede judicial electrónica, será el responsable de la veracidad e integridad de su contenido.

2. La sede judicial electrónica establecerá los medios necesarios para que el ciudadano conozca si la información o servicio al que accede corresponde a la propia sede o a un punto de acceso que no tiene el carácter de sede o a un tercero.

Artículo 13. *Punto de acceso general de la Administración de Justicia.*

1. El punto de acceso general de la Administración de Justicia contendrá el directorio de las sedes judiciales electrónicas que, en este ámbito, faciliten el acceso a los servicios, procedimientos e informaciones accesibles correspondientes a la Administración de Justicia, al Consejo General del Poder Judicial, a la Fiscalía General del Estado y a los organismos públicos vinculados o dependientes de la misma, así como a las Administraciones con competencias en materia de justicia. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras Administraciones públicas o corporaciones que representen los intereses de los profesionales de la justicia, mediante la celebración de los correspondientes convenios.

2. El punto de acceso general será creado y gestionado por el Ministerio de Justicia conforme a los acuerdos que se adopten en el Comité técnico estatal de la Administración judicial electrónica, para asegurar la completa y exacta incorporación de la información y accesos publicados en éste.

CAPÍTULO II

De la identificación y autenticación

Sección 1.ª Disposiciones comunes

Artículo 14. *Formas de identificación y autenticación.*

1. La Administración de Justicia admitirá, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y resulten adecuados para garantizar la identificación de los firmantes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. Sin perjuicio de lo dispuesto en los artículos 4 y 6 de la presente Ley y en todo caso, con sujeción estricta a lo dispuesto por las leyes procesales, los ciudadanos y profesionales

del ámbito de la Justicia podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con la Administración de Justicia:

a) Los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.
b) Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones públicas.
c) Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

3. La Administración de Justicia podrá utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzca:

a) Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede judicial electrónica y el establecimiento con ella de comunicaciones seguras.
b) Sistemas de firma electrónica para la actuación judicial automatizada.
c) Firma electrónica del personal al servicio de la Administración de Justicia.
d) Sistemas de intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo que específicamente se haya convenido.

Artículo 15. *Identificación de las personas jurídicas y entidades sin personalidad jurídica y autenticación de su actuación.*

Las personas jurídicas y entidades sin personalidad jurídica podrán utilizar sistemas de firma electrónica de persona jurídica o de entidades sin personalidad jurídica para todos aquellos procedimientos y actuaciones ante la Administración de Justicia en los términos establecidos en las leyes procesales.

Artículo 16. *Régimen de uso de la firma electrónica.*

1. El uso de la firma electrónica no excluye la obligación de incluir en el documento o comunicación electrónica los datos de identificación que sean necesarios de acuerdo con la legislación aplicable.
2. Los órganos de la Administración de Justicia u organismos públicos vinculados o dependientes podrán tratar los datos personales consignados, a los solos efectos de la verificación de la firma.

Artículo 17. *Régimen de sustitución y habilitación entre profesionales.*

El régimen de acceso a los servicios electrónicos en el ámbito de la Administración de Justicia para los supuestos de sustitución entre profesionales, así como para la habilitación de sus empleados, se regulará por la respectiva Administración competente mediante disposiciones reglamentarias.

Sección 2.ª Identificación electrónica de los órganos judiciales y autenticación del ejercicio de su competencia

Artículo 18. *Identificación de las sedes judiciales electrónicas.*

1. Las sedes judiciales electrónicas utilizarán, para identificarse y garantizar una comunicación segura con las mismas, sistemas de firma electrónica basados en certificados de dispositivo seguro o medio equivalente.
2. Las direcciones electrónicas de la Administración de Justicia y de los organismos públicos vinculados o dependientes de la misma que tengan la condición de sedes judiciales electrónicas deberán hacerlo constar de forma visible e inequívoca.

3. El instrumento de creación de la sede judicial electrónica será accesible directamente o mediante enlace a su publicación en el «Boletín Oficial del Estado» o en el de la Comunidad Autónoma correspondiente.

4. Los sistemas de información que soporten las sedes judiciales electrónicas deberán asegurar la confidencialidad, disponibilidad e integridad de las informaciones que manejan. El Esquema judicial de interoperabilidad y seguridad establecerá las previsiones necesarias para ello, en el marco de la colaboración entre el Consejo General del Poder Judicial, el Ministerio de Justicia, la Fiscalía General del Estado y las Comunidades Autónomas con competencias en materia de justicia.

Artículo 19. *Sistemas de firma electrónica para la actuación judicial automatizada.*

1. Para la identificación y la autenticación del ejercicio de la competencia en la actuación judicial automatizada, la Administración competente facilitará a cada una de las oficinas judiciales del ámbito de su competencia los siguientes sistemas de firma electrónica:

a) Sello electrónico de la oficina judicial basado en certificado electrónico que reúna los requisitos exigidos por la legislación de firma electrónica.

b) Código seguro de verificación vinculado a cada oficina judicial, permitiéndose en todo caso la comprobación de la integridad del documento mediante el acceso a la sede judicial electrónica correspondiente.

2. Los certificados electrónicos a los que se hace referencia en la letra a) del apartado 1 incluirán la denominación correspondiente, pudiendo contener la identidad de la persona titular en el caso de los sellos electrónicos de oficina judicial.

3. La relación de sellos electrónicos utilizados por la Administración de Justicia, incluyendo las características de los certificados electrónicos y los prestadores que los expiden, deberá ser pública y accesible por medios electrónicos. Además, cada Administración competente adoptará las medidas adecuadas para facilitar la verificación de sus sellos electrónicos.

Artículo 20. *Sistemas de firma electrónica mediante sello electrónico.*

1. La creación de sellos electrónicos se realizará mediante resolución de la autoridad competente, que se publicará en la sede judicial electrónica correspondiente y en la que deberá constar:

a) Organismo u órgano titular del sello, que será el responsable de su utilización, con indicación de su adscripción en la Administración de Justicia u organismo público dependiente de la misma.

b) Características técnicas generales del sistema de firma y certificado aplicable.

c) Servicio de validación para la verificación del certificado.

d) Actuaciones y documentos en los que podrá ser utilizado.

2. Los certificados de sello electrónico tendrán, al menos, los siguientes contenidos:

a) Descripción del tipo de certificado, con la denominación «sello electrónico».

b) Nombre del suscriptor.

c) Número de identificación judicial.

3. El modo de emitir los certificados electrónicos de sello electrónico y sus contenidos se definirán en el Esquema judicial de interoperabilidad y seguridad.

Artículo 21. *Firma electrónica de magistrados, jueces, secretarios judiciales, fiscales, abogados del estado y funcionarios al servicio de la Administración de Justicia y otros entes públicos.*

1. Sin perjuicio de lo previsto en los artículos 9 y 10 sobre la sede judicial electrónica, la identificación y autenticación del ejercicio de la competencia de la oficina judicial actuante, cuando utilice medios electrónicos, se realizará mediante firma electrónica del personal a su servicio, de acuerdo con lo dispuesto en los siguientes apartados.

2. Las Administraciones, en el ámbito de sus competencias, proveerán a secretarios judiciales, fiscales, forenses y demás personal al servicio de la Administración de Justicia, de sistemas de firma electrónica, los cuales podrán identificar de forma conjunta al titular del puesto de trabajo y el cargo e identificar también a la oficina u órgano judicial en la que presta sus servicios.

El Ministerio de Justicia facilitará a las Administraciones competentes datos actualizados de los fiscales y secretarios judiciales a fin de dotarles de firma electrónica.

3. Los sistemas de firma electrónica de jueces y magistrados serán los que provea el Consejo General del Poder Judicial. Este podrá establecer, a través de convenios, que el proveedor sea la Administración competente.

4. Las Administraciones, en el ámbito de sus competencias, dotarán de sistemas de firma electrónica a los representantes procesales del Estado y demás entes públicos, a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Sección 3.ª De la interoperabilidad y de la acreditación y representación de los ciudadanos

Artículo 22. *Interoperabilidad de la identificación y autenticación por medio de certificados electrónicos.*

1. Los certificados electrónicos reconocidos emitidos por prestadores de servicios de certificación serán admitidos por la Administración de Justicia como válidos en las relaciones con la misma, siempre y cuando el prestador de servicios de certificación ponga a disposición de las Administraciones competentes en materia de justicia la información que se precise en condiciones que resulten tecnológicamente viables, bajo principios de reconocimiento mutuo y reciprocidad y sin que suponga coste alguno para aquéllas.

2. Las Administraciones competentes dispondrán de acceso, al menos, a alguna plataforma de verificación del estado de revocación de todos los certificados admitidos en el ámbito de la Administración de Justicia, que será de libre acceso por parte de todos los órganos judiciales.

Artículo 23. *Identificación y autenticación de los ciudadanos por funcionario público.*

1. En los supuestos en que para la realización de cualquier actuación por medios electrónicos se requiera la identificación o autenticación del ciudadano mediante algún instrumento de los previstos en el artículo 14 de los que aquél no disponga, tal identificación o autenticación será válidamente realizada por un funcionario mediante el uso del sistema de firma electrónica del que esté dotado.

2. Para la eficacia de lo dispuesto en el apartado anterior, el ciudadano deberá identificarse y prestar su consentimiento expreso, debiendo quedar constancia de ello para los casos de discrepancia o litigio.

Artículo 24. *Intercambio electrónico de datos en entornos cerrados de comunicación.*

1. Los documentos electrónicos transmitidos en entornos cerrados de comunicaciones establecidos entre Administraciones con competencias en materia de justicia, órganos y entidades de derecho público, serán considerados válidos a efectos de autenticación e identificación de los emisores y receptores en las condiciones establecidas en el presente artículo.

2. Cuando los participantes en las comunicaciones pertenezcan a la Administración de Justicia, el Comité técnico estatal de la Administración judicial electrónica determinará las condiciones y garantías por las que se regirán, que al menos comprenderán la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

3. Cuando los participantes pertenezcan a distintas Administraciones o a entidades de derecho público, las condiciones y garantías citadas en el apartado anterior se establecerán mediante convenio.

4. En todo caso deberá garantizarse la seguridad del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

TÍTULO IV

De la tramitación electrónica de los procedimientos judiciales

CAPÍTULO I

Disposiciones comunes

Artículo 25. *Criterios para la gestión electrónica.*

1. La gestión electrónica de la actividad judicial respetará el cumplimiento de los requisitos formales y materiales establecidos en las normas procesales. A estos efectos se impulsará la aplicación de medios electrónicos a los procesos de trabajo y a la gestión de los procedimientos y de la actuación judicial.

2. La aplicación de medios electrónicos a la gestión de los procedimientos, procesos y servicios irá siempre precedida de la realización por el Comité técnico estatal de la Administración judicial electrónica de un análisis de rediseño funcional y simplificación del procedimiento, proceso o servicio, en el que se considerarán especialmente los siguientes aspectos:

a) La posible supresión o reducción de la documentación requerida a los ciudadanos, mediante su sustitución por datos, transmisiones de datos o certificaciones.

b) La reducción de los tiempos en la tramitación de los procedimientos.

c) La racionalización de la distribución de las cargas de trabajo y de las comunicaciones internas y la introducción de indicadores de gestión.

CAPÍTULO II

Del expediente judicial electrónico

Artículo 26. *Expediente judicial electrónico.*

1. El expediente judicial electrónico es el conjunto de datos, documentos, trámites y actuaciones electrónicas, así como de grabaciones audiovisuales correspondientes a un procedimiento judicial, cualquiera que sea el tipo de información que contenga y el formato en el que se hayan generado.

2. Se asignará un número de identificación general a aquellos documentos que puedan generar un nuevo procedimiento, que será único e inalterable a lo largo de todo el proceso, permitiendo su identificación unívoca por cualquier órgano del ámbito judicial en un entorno de intercambio de datos.

3. El foliado de los expedientes judiciales electrónicos se llevará a cabo mediante un índice electrónico, firmado por la oficina judicial actuante, según proceda. Este índice garantizará la integridad del expediente judicial electrónico y permitirá su recuperación siempre que sea preciso, siendo admisible que un mismo documento forme parte de distintos expedientes judiciales electrónicos.

4. La remisión de expedientes se sustituirá a todos los efectos legales por la puesta a disposición del expediente judicial electrónico, teniendo derecho a obtener copia electrónica del mismo todos aquellos que lo tengan conforme a lo dispuesto en las normas procesales.

Artículo 27. *Documento judicial electrónico.*

1. Tendrán la consideración de documentos judiciales electrónicos las resoluciones y actuaciones que se generen en los sistemas de gestión procesal, así como toda información que tenga acceso de otra forma al expediente, cuando incorporen datos firmados electrónicamente en la forma prevista en la Sección 2.ª del Capítulo II del Título III de la presente Ley.

2. Las Administraciones competentes, en su relación de prestadores de servicios de certificación electrónica, especificarán aquellos que con carácter general estén admitidos para prestar servicios de sellado de tiempo.

3. Tendrá la consideración de documento público el documento electrónico que incluya la fecha electrónica y que incorpore la firma electrónica reconocida del secretario judicial, siempre que actúe en el ámbito de sus competencias, conforme a lo dispuesto en las leyes procesales.

Artículo 28. *Copias electrónicas.*

1. Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las oficinas judiciales, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en las leyes procesales, siempre que el documento electrónico original se encuentre en poder de la oficina judicial donde haya sido originado o incorporado y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento.

Si se alterase el formato original, deberá incluirse en los metadatos la condición de copia.

2. Las copias realizadas por las oficinas judiciales, utilizando medios electrónicos, de documentos emitidos originalmente por ellas en soporte papel tendrán la consideración de copias auténticas.

3. Las oficinas judiciales podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico.

4. A los documentos emitidos originalmente en soporte papel de los que se hayan efectuado copias electrónicas de acuerdo con lo dispuesto en este artículo, se les dará el destino previsto en la normativa vigente en materia de archivos judiciales.

5. Las copias realizadas en soporte papel de documentos judiciales electrónicos y firmados electrónicamente por el secretario judicial tendrán la consideración de copias auténticas, siempre que incluyan la impresión de un código seguro de verificación que permita contrastar su autenticidad mediante el acceso a los archivos electrónicos de la oficina judicial emisora.

Artículo 29. *Archivo electrónico de documentos.*

1. Podrán almacenarse por medios electrónicos todos los documentos utilizados en las actuaciones judiciales.

Los Archivos Judiciales de Gestión, Territoriales y Central serán gestionados mediante programas y aplicaciones informáticas, compatibles con los ya existentes en juzgados y tribunales, adaptados a las funciones y cometidos de cada uno, cuyo funcionamiento electrónico será regulado mediante Real Decreto.

2. Los documentos electrónicos que contengan actos procesales que afecten a derechos o intereses de los particulares deberán conservarse en soportes de esta naturaleza, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure la identidad e integridad de la información necesaria para reproducirlo. Se asegurará en todo caso la posibilidad de trasladar los datos a otros formatos y soportes que garanticen el acceso desde diferentes aplicaciones.

3. Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados y ajustarse a los requerimientos que garanticen la compatibilidad e interoperabilidad de los sistemas informáticos. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como lo previsto en los artículos 234 y 235 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en las leyes procesales.

4. Sin perjuicio de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, el Consejo General del Poder Judicial regulará reglamentariamente la reutilización de sentencias y otras resoluciones judiciales por medios

digitales de referencia o reenvío de información, sea o no con fines comerciales, por parte de personas físicas o jurídicas para facilitar el acceso a las mismas de terceras personas.

CAPÍTULO III

Del registro de escritos, las comunicaciones y las notificaciones electrónicas

Sección 1.ª Del registro de escritos

Artículo 30. *Registro judicial electrónico.*

1. Las Administraciones competentes dotarán a las oficinas judiciales con funciones de registro de los medios electrónicos adecuados para la recepción y registro de escritos y documentos, traslado de copias, realización de actos de comunicación y expedición de resguardos electrónicos a través de medios de transmisión seguros, entre los que se incluirán los sistemas de firma y sellado de tiempo electrónicos reconocidos.

2. Los registros judiciales electrónicos creados en las condiciones del apartado anterior se corresponderán con la subsede judicial electrónica.

3. En estos registros judiciales electrónicos únicamente se admitirán escritos y documentos dirigidos a las oficinas judiciales dependientes del mismo, conforme a lo establecido en el artículo 230 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y en las leyes procesales.

4. La recepción de solicitudes, escritos y comunicaciones podrá interrumpirse por el tiempo imprescindible sólo cuando concurran razones justificadas de mantenimiento técnico u operativo. La interrupción deberá anunciarse a los potenciales usuarios del registro electrónico con la antelación que, en cada caso, resulte posible.

En supuestos de interrupción no planificada en el funcionamiento del registro electrónico, y siempre que sea posible, se dispondrán las medidas para que el usuario resulte informado de esta circunstancia, así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. Alternativamente, podrá establecerse un redireccionamiento que permita utilizar un registro electrónico en sustitución de aquél en el que se haya producido la interrupción.

Artículo 31. *Funcionamiento.*

1. Los registros electrónicos emitirán automáticamente un recibo consistente en una copia autenticada del escrito, documento o comunicación de que se trate, incluyendo la fecha y hora de presentación y el número de entrada de registro.

2. Los documentos que se acompañen al correspondiente escrito o comunicación, deberán cumplir los estándares de formato y requisitos de seguridad que se determinen en el marco institucional de cooperación en materia de administración electrónica. Los registros electrónicos generarán recibos acreditativos de la entrega de estos documentos que garanticen la integridad y el no repudio de los documentos aportados, así como la fecha y hora de presentación y el número de registro de entrada en la correspondiente sede judicial electrónica.

Artículo 32. *Cómputo de plazos.*

1. Los registros electrónicos se regirán a efectos de cómputo de los plazos imputables tanto a los interesados como a las oficinas judiciales por la fecha y hora oficial de la sede judicial electrónica de acceso, que deberá contar con las medidas de seguridad necesarias para garantizar su integridad y figurar visible.

2. Los registros electrónicos permitirán la presentación de escritos, documentos y comunicaciones todos los días del año durante las veinticuatro horas.

3. A los efectos del cómputo de plazo fijado en días hábiles o naturales, y en lo que se refiere a cumplimiento de plazos por los interesados, la presentación, en un día inhábil a efectos procesales conforme a la ley, se entenderá realizada en la primera hora del primer día hábil siguiente, salvo que una norma permita expresamente la recepción en día inhábil.

4. El inicio del cómputo de los plazos que hayan de cumplir las oficinas judiciales vendrá determinado por la fecha y hora de presentación en el propio registro.

5. Cada sede judicial electrónica en la que esté disponible un registro electrónico determinará, atendiendo al ámbito territorial en el que ejerce sus competencias el titular de aquélla, los días que se considerarán inhábiles a los efectos de los apartados anteriores.

Artículo 32 bis. *Archivos electrónicos de apoderamientos apud acta.*

1. Asimismo, se dispondrá en las oficinas judiciales con funciones de registro, de un archivo electrónico de apoderamientos en el que deberán inscribirse los apoderamientos apud acta otorgados presencial o electrónicamente por quien ostente la condición de interesado en un procedimiento judicial a favor de representante, para actuar en su nombre ante la Administración de Justicia.

Ello no impedirá la existencia de archivos electrónicos de apoderamientos apud acta en cada oficina judicial para la realización de los trámites específicos en cada una.

2. Los archivos electrónicos de apoderamientos apud acta deberán ser plenamente interoperables entre sí, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se registren en sus correspondientes archivos.

Los archivos electrónicos de apoderamientos apud acta permitirán comprobar válidamente la representación que ostentan quienes actúen ante la Administración de Justicia en nombre de un tercero.

3. Los asientos que se realicen en los archivos electrónicos de apoderamientos apud acta deberán contener, al menos, la siguiente información:

a) Nombre y apellidos o razón social, número de documento nacional de identidad, de identificación fiscal o de documento equivalente del poderdante.

b) Nombre y apellidos o razón social, número de documento nacional de identidad, de identificación fiscal o de documento equivalente del apoderado.

c) Fecha de inscripción.

d) Tipo de poder según las facultades que otorgue.

4. Los apoderamientos apud acta que se inscriban en los archivos electrónicos de apoderamientos apud acta deberán corresponder a alguna de las siguientes tipologías:

a) Un poder general para que el apoderado pueda actuar en nombre del poderdante en cualquier actuación judicial.

b) Un poder para que el apoderado pueda actuar en nombre del poderdante únicamente en determinadas clases de procedimientos.

c) Un poder especial para que el apoderado pueda actuar en nombre del poderdante en un procedimiento concreto.

5. El poder inscribible en que la parte otorgue su representación al apoderado habrá de ser conferido por comparecencia apud acta.

El apoderamiento apud acta se otorgará mediante comparecencia electrónica en la correspondiente sede electrónica judicial haciendo uso de los sistemas de firma electrónica previstos en esta Ley, o bien mediante comparecencia personal ante el secretario judicial de cualquier oficina judicial.

6. Los apoderamientos inscritos en el archivo tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción. En todo caso, en cualquier momento antes de la finalización de dicho plazo el poderdante podrá revocar o prorrogar el poder. Las prórrogas otorgadas por el poderdante al apoderamiento tendrán una validez determinada máxima de cinco años a contar desde la fecha de inscripción.

7. Las solicitudes de revocación, de prórroga o de denuncia del mismo podrán dirigirse a cualquier archivo, debiendo quedar inscrita esta circunstancia en el archivo ante el que tenga efectos el poder y surtiendo efectos desde la fecha en la que se produzca dicha inscripción.

Sección 2.ª De las comunicaciones y las notificaciones electrónicas

Artículo 33. *Comunicaciones electrónicas.*

1. Los ciudadanos podrán elegir en todo momento la manera de comunicarse con la Administración de Justicia, sea o no por medios electrónicos.

Asimismo, se podrá establecer legal o reglamentariamente la obligatoriedad de comunicarse con ella utilizando solo medios electrónicos cuando se trate de personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

2. Las comunicaciones a través de medios electrónicos se realizarán, en todo caso, con sujeción a lo dispuesto en la legislación procesal y serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas y del contenido íntegro de las comunicaciones, y se identifique con la autenticación que sea exigible al remitente y al destinatario de las mismas.

3. Las Administraciones competentes en materia de justicia publicarán, en el correspondiente «Diario Oficial» y en la propia sede judicial electrónica, aquellos medios electrónicos que los ciudadanos pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con las oficinas judiciales.

4. Los requisitos de seguridad e integridad de las comunicaciones se establecerán en cada caso de forma apropiada al carácter de los datos objeto de aquellas, de acuerdo con criterios de proporcionalidad, conforme a lo dispuesto en la legislación vigente en materia de protección de datos de carácter personal y en las leyes procesales.

5. Los profesionales de la justicia deberán realizar sus comunicaciones por medios electrónicos cuando técnicamente estén disponibles.

6. Las oficinas judiciales utilizarán en todo caso medios electrónicos en sus comunicaciones con otras Administraciones y organismos públicos, salvo imposibilidad legal o material.

Artículo 34. *Práctica de actos de comunicación por medios electrónicos.*

1. El sistema de notificación permitirá acreditar la fecha y hora en que se produzca la salida y las de la puesta a disposición del interesado del acto objeto de notificación, así como de acceso a su contenido.

2. En caso de que el acto de comunicación no pueda llevarse a cabo por medios electrónicos, se procederá a imprimir la resolución y la documentación necesaria, procediéndose a la práctica del acto de comunicación en la forma establecida en las leyes procesales e incorporándose a continuación el documento acreditativo de la práctica del acto de comunicación, debidamente digitalizado, al expediente judicial electrónico. En todo caso, el destinatario del acto de comunicación tendrá derecho a obtener copia de la documentación recibida en formato electrónico.

Artículo 35. *Comunicación edictal electrónica.*

La publicación de resoluciones y comunicaciones que por disposición legal deban fijarse en tablón de anuncios, así como la publicación de los actos de comunicación procesal que deban ser objeto de inserción en el «Boletín Oficial del Estado», en el de la Comunidad Autónoma o en el de la provincia respectiva, serán sustituidas en todos los órdenes jurisdiccionales por su publicación en el Tablón Edictal Judicial único previsto en el artículo 236 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

El Tablón Edictal Judicial Único será publicado electrónicamente por la Agencia Estatal Boletín Oficial del Estado, en la forma en que se disponga reglamentariamente. A tal efecto, la Agencia Estatal Boletín Oficial del Estado pondrá a disposición de los juzgados y tribunales un sistema automatizado de remisión y gestión telemática que garantizará la celeridad en la publicación de los edictos, su correcta y fiel inserción, así como la identificación del órgano remitente.

CAPÍTULO IV

De la tramitación electrónica

Artículo 36. *Iniciación del procedimiento por medios electrónicos.*

1. La iniciación de un procedimiento judicial por medios electrónicos por los ciudadanos, en aquellos juicios en los que pueden comparecer de forma personal y directa por no ser preceptiva la asistencia letrada ni la representación por procurador conforme a lo establecido en las normas de procedimiento, requerirá la puesta a disposición de los interesados de los correspondientes modelos o impresos normalizados en la sede judicial electrónica, que deberán ser accesibles sin otras restricciones tecnológicas que las estrictamente derivadas de la utilización de estándares y criterios de comunicación y seguridad aplicables de acuerdo con las normas y protocolos nacionales e internacionales.

2. En todo caso, cuando los escritos fueran presentados en papel por las personas a las que se refiere el apartado primero del presente artículo, se procederá a su digitalización por la sección correspondiente del servicio común procesal que tenga atribuidas dichas funciones.

3. Los profesionales de la justicia presentarán sus demandas y otros escritos por vía telemática a través de los sistemas previstos en esta Ley, empleando firma electrónica reconocida.

4. Todo escrito iniciador del procedimiento deberá ir acompañado de un formulario normalizado debidamente cumplimentado en los términos que se establezcan reglamentariamente.

Artículo 37. *Tramitación del procedimiento utilizando medios electrónicos.*

1. Las aplicaciones y sistemas de información utilizados para la gestión por medios electrónicos de los procedimientos deberán garantizar el control de los tiempos y plazos, la identificación del órgano u oficina responsable de los procedimientos, así como la tramitación ordenada de los expedientes, y facilitar la simplificación y la publicidad de los procedimientos.

2. Los sistemas de comunicación utilizados en la gestión electrónica de los procedimientos para las comunicaciones entre las unidades intervinientes en la tramitación de las distintas fases del proceso deberán cumplir los requisitos establecidos en esta Ley y en las disposiciones reglamentarias de desarrollo.

3. Cuando se utilicen medios electrónicos en la gestión del procedimiento, los actos de comunicación y notificación que hayan de practicarse se realizarán conforme a las disposiciones contenidas en los artículos 33 a 35 de esta Ley.

4. Los expedientes y demás actuaciones que deban ser remitidos por otras Administraciones y organismos públicos deberán realizarse en todo caso por vía telemática a través de la correspondiente sede judicial electrónica. El expediente administrativo electrónico habrá de cumplir los requisitos previstos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, y deberá remitirse debidamente foliado mediante un índice electrónico que permita la debida localización y consulta de los documentos incorporados.

Artículo 38. *Presentación de escritos, documentos u otros medios o instrumentos.*

1. La presentación de toda clase de escritos, documentos, dictámenes, informes u otros medios o instrumentos se ajustará a lo dispuesto en las leyes procesales, debiendo ir acompañados en todo caso del formulario normalizado a que se refiere el apartado 4 del artículo 36, en el que además se consignará el tipo y número de expediente y año al que se refiera el escrito.

2. En todo caso, la presentación de escritos, documentos y otros medios o instrumentos se ajustará a las siguientes reglas:

a) Los documentos en papel que, conforme a lo dispuesto en las leyes procesales puedan o deban ser aportados por las partes en cualquier momento del procedimiento, deberán ser incorporados como anexo al documento principal mediante imagen digitalizada

de la copia, si fueran públicos, o del original del documento obrante en papel, si se tratara de documentos privados. El archivo de la imagen digitalizada habrá de ir firmado mediante la utilización de los sistemas de firma electrónica previstos en la presente Ley, en las leyes procesales o en otras normas de desarrollo.

b) Los documentos electrónicos públicos o privados se incorporarán como anexo al documento principal siguiendo los sistemas previstos en esta Ley o en sus normas de desarrollo y conforme a lo previsto en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

c) En caso de que fueran impugnados por la parte contraria, se procederá conforme a lo dispuesto en las leyes procesales y, en su caso, en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

d) No se admitirá la aportación en otra forma, salvo en el supuesto de que, por las singularidades características del documento, el sistema no permita su incorporación como anexo para su envío por vía telemática. En estos casos, el usuario hará llegar dicha documentación al destinatario por otros medios en la forma que establezcan las normas procesales, y deberá hacer referencia a los datos identificativos del envío telemático al que no pudo ser adjuntada, presentando el original ante el órgano judicial en el día siguiente hábil a aquel en que se hubiera efectuado el envío telemático. Tales documentos serán depositados y custodiados por quien corresponda en el archivo, de gestión o definitivo, de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia únicamente en formato papel.

Cuando se deban incorporar documentos sobre los cuales existan sospechas de falsedad, deberá aportarse en todo caso además el documento original, al que se le dará el tratamiento contemplado en el párrafo anterior.

e) En los casos en que se deban aportar al procedimiento medios o instrumentos de prueba que por su propia naturaleza no sean susceptibles de digitalización, serán depositados y custodiados por quien corresponda en el archivo de gestión o definitivo de la oficina judicial, dejando constancia en el expediente judicial electrónico de su existencia.

Artículo 39. *Traslado de copias.*

El traslado de copias por vía telemática se realizará de forma simultánea a la presentación telemática de escritos y documentos ante el órgano u oficina judicial correspondiente.

Artículo 40. *Acreditación de la representación procesal.*

1. Se aportará copia electrónica del poder notarial de representación conferido al procurador. En caso de impugnación, el secretario judicial procederá a comprobar el apoderamiento a través de la Agencia Notarial de Certificación.

2. La representación otorgada por comparecencia apud-acta ante secretario judicial se acreditará adjuntando copia electrónica de la misma o mediante indicación del número, fecha y secretario judicial ante quien se otorgó.

3. El apoderamiento podrá igualmente acreditarse mediante la certificación de su inscripción en el archivo electrónico de apoderamientos apud acta de las oficinas judiciales.

Artículo 41. *Acceso de las partes a la información sobre el estado de tramitación.*

Se pondrá a disposición de las partes un servicio electrónico de acceso restringido donde éstas puedan consultar, previa identificación y autenticación, al menos la información sobre el estado de tramitación del procedimiento, salvo que la normativa aplicable establezca restricciones a dicha información y con pleno respeto a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y legislación que la desarrolla. La información sobre el estado de tramitación del procedimiento comprenderá la relación de los actos de trámite realizados, con indicación sobre su contenido, así como la fecha en la que fueron dictados.

Artículo 42. *Actuación judicial automatizada.*

En caso de actuación automatizada, deberá establecerse previamente por el Comité técnico estatal de la Administración judicial electrónica la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso la auditoría del sistema de información y de su código fuente.

Los sistemas incluirán los indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica, cada uno en el ámbito de sus competencias.

Artículo 43. *Subsanación de actos procesales.*

1. El incumplimiento del deber de uso de las tecnologías, en los términos establecidos en esta Ley, por un profesional de la justicia en su primera comunicación con un órgano judicial podrá ser subsanado. A estos efectos, el órgano judicial concederá un plazo máximo de cinco días con apercibimiento de que todas sus actuaciones ante ese órgano, en ese o en cualquier otro proceso, así como ante cualquier otro órgano del mismo partido judicial, deberán realizarse empleando medios electrónicos y de conformidad con esta Ley.

2. Si la subsanación no se efectuase en el plazo señalado en el anterior apartado, no se admitirá la actuación que se tratara de realizar.

3. No será preciso practicar el requerimiento a que se refiere el apartado 1 del presente artículo cuando el profesional hubiera sido requerido en tal sentido por cualquier otro órgano judicial del mismo partido judicial, rechazándose de plano cualquier actuación que se tratara de efectuar por medios distintos a los previstos en la presente Ley.

TÍTULO V

Cooperación entre las Administraciones con competencias en materia de Administración de Justicia. El Esquema judicial de interoperabilidad y seguridad

CAPÍTULO I

Marco institucional de cooperación en materia de administración electrónica

Artículo 44. *El Comité técnico estatal de la Administración judicial electrónica.*

1. El Comité técnico estatal de la Administración judicial electrónica estará integrado por una representación del Ministerio de Justicia y de cada una de las Comunidades Autónomas con competencias en la materia y por los representantes que al efecto podrán designar el Consejo General del Poder Judicial y la Fiscalía General del Estado.

Este Comité técnico estará copresidido por un representante del Consejo General del Poder Judicial y otro del Ministerio de Justicia.

2. Sin perjuicio de las competencias del Consejo General del Poder Judicial como garante de la compatibilidad de sistemas informáticos, este Comité tendrá las siguientes funciones:

a) Favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados por la Administración de Justicia.

b) Preparar planes y programas conjuntos de actuación para impulsar el desarrollo de la Administración judicial electrónica, respetando en todo caso las competencias autonómicas atinentes a los medios materiales de la Administración de Justicia.

c) Promover la cooperación de otras Administraciones públicas con la Administración de Justicia para suministrar a los órganos judiciales, a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, la información que precisen en el curso de un proceso judicial en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y en las leyes procesales.

d) Aquellas otras que legalmente se determinen.

Artículo 45. *Funcionamiento integrado y conjunto de todas las aplicaciones informáticas.*

El Comité técnico estatal de la Administración judicial electrónica fijará las bases para el desarrollo del Esquema judicial de interoperabilidad y seguridad de modo que permita, a través de las plataformas tecnológicas necesarias, la interoperabilidad total de todas las aplicaciones informáticas al servicio de la Administración de Justicia.

CAPÍTULO II

Esquema judicial de interoperabilidad y seguridad

Sección 1.ª Interoperabilidad judicial

Artículo 46. *Interoperabilidad de los sistemas de información.*

1. La Administración de Justicia utilizará las tecnologías de la información aplicando medidas informáticas, tecnológicas, organizativas y de seguridad que aseguren un adecuado nivel de interoperabilidad técnica, semántico-jurídica y organizativa entre todos los sistemas y aplicaciones que prestan servicios a la Administración de Justicia.

2. En el desarrollo de la actividad de la oficina judicial será obligatorio el uso de los servicios y consultas ofrecidos a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, salvo que existan razones técnicas que impidan su utilización.

Los programas y aplicaciones informáticos que se utilicen en la Administración de Justicia deberán ser previamente aprobados por el Consejo General del Poder Judicial, a los efectos de asegurar su compatibilidad con las funciones que le encomienda el artículo 230.5 de la Ley Orgánica del Poder Judicial.

Artículo 47. *Esquema judicial de interoperabilidad y seguridad.*

1. El Esquema judicial de interoperabilidad y seguridad será aplicado en la Administración de Justicia para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

2. El Esquema judicial de interoperabilidad y seguridad comprenderá:

a) El conjunto de criterios y recomendaciones en materia de seguridad, conservación, normalización y volcado de datos de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las distintas instituciones y Administraciones competentes para la toma de decisiones tecnológicas que aseguren la interoperabilidad.

b) La política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley y el establecimiento de los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3. En su elaboración se tendrá en cuenta lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones competentes en materia de justicia y los servicios electrónicos e infraestructuras ya existentes. A estos efectos utilizarán preferentemente estándares abiertos, así como, en su caso y de forma complementaria, considerarán el uso de estándares que sean de uso generalizado por los ciudadanos.

Artículo 48. *La interoperabilidad y la seguridad como cualidades integrales.*

1. Tanto la interoperabilidad como la seguridad se tendrán presentes de forma integral desde la concepción de los servicios, sistemas y aplicaciones a lo largo de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, publicación, conservación y acceso o interconexión con los mismos.

2. En el caso de la seguridad judicial, se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con el sistema, atendiendo en todo caso a la especial sensibilidad de la información contenida en los procedimientos judiciales electrónicos.

Artículo 49. *Normas de conformidad.*

1. La interoperabilidad y la seguridad de las sedes y registros judiciales electrónicos, así como las del acceso electrónico de los ciudadanos a los servicios judiciales, se regirán por lo establecido en la presente Ley.
2. La conformidad con el Esquema judicial de interoperabilidad y seguridad se incluirá en el ciclo de vida de los servicios y sistemas, acompañada de los correspondientes procedimientos de control.
3. El Comité técnico estatal de Administración judicial electrónica velará por el establecimiento de los mecanismos de control para asegurar, de forma efectiva, el cumplimiento del Esquema judicial de interoperabilidad y seguridad.
4. En las sedes judiciales electrónicas correspondientes se publicarán las declaraciones de conformidad, compatibilidad y otros posibles distintivos de interoperabilidad obtenidos respecto al cumplimiento del Esquema judicial de interoperabilidad y seguridad.

Artículo 50. *Mejora continua del proceso de seguridad.*

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a gestión de las tecnologías de la información.

Artículo 51. *Desarrollo del marco normativo técnico.*

Para el mejor cumplimiento de lo establecido en relación con el Esquema judicial de interoperabilidad y seguridad, el Comité técnico estatal de la Administración judicial electrónica, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones. El Consejo General del Poder Judicial aprobará las guías cuando afecten a la compatibilidad de los sistemas informáticos en los términos previstos en el artículo 230.5 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

Artículo 52. *Actualización permanente.*

1. El Esquema judicial de interoperabilidad y seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de administración electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que lo apoyan. Para ello, se desarrollarán las correspondientes guías y normas técnicas de aplicación.
2. Corresponde al Comité técnico estatal de la Administración judicial electrónica aprobar las bases para la actualización del Esquema judicial de interoperabilidad y seguridad.

Sección 2.ª Seguridad judicial electrónica

Artículo 53. *Elementos básicos de la seguridad judicial electrónica.*

1. En las decisiones en materia de seguridad judicial electrónica deberán tenerse en cuenta los siguientes elementos:

a) La seguridad integral, desde el punto de vista de un proceso integral constituido por los elementos organizativos, normativos, humanos y técnicos relacionados con el sistema.
b) La gestión de riesgos, como proceso de garantía de la seguridad de la información.
c) La prevención, detección, reacción, corrección y recuperación como procesos soporte a la seguridad de la información.
d) Los niveles de seguridad, entendidos como capas de seguridad que permitan una gestión de incidentes más adecuada.

e) La reevaluación periódica de las medidas de seguridad existentes para adecuar su eficacia a la constante evolución de riesgos, tecnología y sistemas de protección.

f) La función diferenciada dentro de la organización, estableciendo una estructura organizativa donde se identifiquen las figuras de responsable de la información, responsable de seguridad y responsable del servicio prestado.

2. Son dimensiones de la seguridad judicial electrónica:

a) Autenticidad.
b) Confidencialidad.
c) Integridad.
d) Disponibilidad.
e) Trazabilidad.
f) Conservación.

Artículo 54. *Requisitos mínimos de seguridad.*

El Esquema judicial de interoperabilidad y seguridad fijará los requisitos mínimos que todas las instituciones judiciales han de garantizar en relación a los sistemas de información de los que son responsables. Estos requisitos se desarrollarán mediante una guía técnica.

CAPÍTULO III

Reutilización de aplicaciones y transferencia de tecnologías. Directorio general de información tecnológica judicial

Artículo 55. *Reutilización de sistemas, infraestructuras y aplicaciones de propiedad de las Administraciones de Justicia.*

1. Las Administraciones titulares de los derechos de propiedad intelectual de aplicaciones, desarrolladas por sus servicios o cuyo desarrollo haya sido objeto de contratación, podrán ponerlas a disposición de cualquier institución judicial o cualquier Administración pública sin contraprestación y sin necesidad de convenio.

2. Las aplicaciones a las que se refiere el apartado anterior podrán ser declaradas como de fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración de Justicia. Se publicarán, en tal caso, como licencia pública de la Unión Europea, sin perjuicio de otras licencias que aseguren que los programas, datos o información que se comparten:

a) Pueden ejecutarse para cualquier propósito.
b) Permiten conocer su código fuente.
c) Pueden modificarse o mejorarse.
d) Pueden redistribuirse a otros usuarios con o sin cambios, siempre que la obra derivada mantenga estas mismas cuatro garantías.

3. En el desarrollo de las soluciones para la Administración de Justicia se fomentará la reutilización de los sistemas, servicios, infraestructuras y aplicaciones existentes, siempre que los requisitos tecnológicos de interoperabilidad y seguridad así lo permitan.

Artículo 56. *Transferencia de tecnología entre Administraciones. Directorio General de información tecnológica judicial.*

1. El Ministerio de Justicia mantendrá un directorio general de aplicaciones judiciales para su reutilización e impulsará el mantenimiento del mismo, en colaboración con el resto de Administraciones competentes en materia de justicia. Se promoverá el desarrollo de guías técnicas, formatos y estándares comunes de especial interés para el desarrollo de la Administración judicial electrónica en el marco institucional de cooperación en materia de administración electrónica.

2. Las Administraciones mantendrán directorios actualizados de aplicaciones para su libre reutilización, especialmente en aquellos campos de especial interés para el desarrollo

de la administración electrónica y de conformidad con lo que al respecto se establezca en el marco institucional de cooperación en materia de administración electrónica.

3. Las instituciones judiciales deberán tener en cuenta las soluciones disponibles para la libre reutilización que puedan satisfacer total o parcialmente las necesidades de los nuevos sistemas y servicios o la mejora y actualización de los ya implantados.

Disposición adicional primera. *Creación del Comité técnico estatal de la Administración judicial electrónica.*

La estructura, composición y funciones del Comité técnico estatal de la Administración judicial electrónica serán establecidas reglamentariamente por el Gobierno, mediante Real Decreto, previo informe del Consejo General del Poder Judicial, de la Fiscalía General del Estado, de la Agencia Española de Protección de Datos y de las Comunidades Autónomas con competencias en la materia.

Disposición adicional segunda. *Adaptación a los sistemas de administración electrónica.*

Para garantizar la efectividad del derecho a la tutela judicial reconocida en el artículo 24 de la Constitución, en el plazo de cinco años desde la entrada en vigor de esta Ley las Administraciones con competencia en materia de Administración de Justicia dotarán a las oficinas judiciales y fiscalías de sistemas de gestión procesal que permitan la tramitación electrónica de los procedimientos.

Disposición adicional tercera. *Interoperabilidad entre las aplicaciones de la Administración de Justicia.*

En el plazo de cuatro años desde la entrada en vigor de la presente Ley, las Administraciones con competencia en materia de Administración de Justicia garantizarán la interoperabilidad entre los sistemas al servicio de la Administración de Justicia, de acuerdo a las especificaciones establecidas por el Comité técnico estatal de Administración judicial electrónica en el marco institucional de cooperación en materia de administración electrónica.

Disposición adicional cuarta. *Accesibilidad a los servicios electrónicos.*

Las Administraciones con competencias en materia de justicia garantizarán que todos los ciudadanos, con especial atención a las personas mayores o con algún tipo de discapacidad, que se relacionan con la Administración de Justicia puedan acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos. Las características de los medios que permitan la universalización del acceso a los servicios electrónicos serán desarrolladas reglamentariamente por el Gobierno, mediante Real Decreto, previo informe de las Comunidades Autónomas con competencias en la materia.

Disposición adicional quinta. *Dotación de medios e instrumentos electrónicos y sistemas de información.*

Las Administraciones competentes en materia de Justicia dotarán a todos los órganos, oficinas judiciales y fiscalías de los medios e instrumentos electrónicos y de los sistemas de información necesarios y suficientes para poder desarrollar su función eficientemente. Estos sistemas serán plenamente accesibles y operativos sin necesidad de que los usuarios se encuentren físicamente en las sedes de sus respectivos órganos, oficinas o fiscalías, con respeto a las políticas internas que garanticen el derecho a la desconexión digital recogido en el artículo 14.j.bis y en el artículo 88 del texto refundido de la Ley del Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre. Asimismo, formarán a los integrantes de los mismos en el uso y utilización de dichos medios e instrumentos.

Disposición adicional sexta. *Representantes procesales del Estado y demás entes públicos.*

1. A los efectos señalados en el artículo 24, y, en general, de aplicación de esta Ley a la actuación procesal de los abogados del Estado, representantes procesales del Estado y demás entes públicos a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, se suscribirá un protocolo de actuación.

2. Las Administraciones competentes en materia de justicia dotarán a los órganos y oficinas de los representantes del Estado y demás entes públicos a los que se refiere el artículo 551 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, de los medios e instrumentos electrónicos necesarios y suficientes para poder desarrollar su función eficientemente. Asimismo, formarán a los integrantes de los mismos en el uso y utilización de dichos medios e instrumentos.

Disposición adicional séptima. *Legislación aplicable.*

La presente Ley tiene carácter transversal para todos los órdenes jurisdiccionales y complementará la legislación vigente en lo concerniente al uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Disposición adicional octava. *Legislación aplicable en materia de interoperabilidad.*

En lo no previsto en esta Ley, los criterios de interoperabilidad para las relaciones entre la Administración de Justicia y las Administraciones públicas, así como las entidades sujetas a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, se regirán conforme a lo contemplado en esta última.

Disposición adicional novena. *Aplicación de la Ley al Ministerio Fiscal.*

Las referencias contenidas en el texto y articulado de la presente Ley a las oficinas judiciales, actividad judicial, juzgados y tribunales, sede judicial electrónica, órganos judiciales, expediente judicial electrónico, documento judicial electrónico, registro judicial electrónico y procedimiento judicial, serán de aplicación equivalente y se entenderán referidas igualmente a las oficinas fiscales, actividad fiscal, fiscalías, sedes fiscales electrónicas, expedientes fiscales electrónicos, registros fiscales electrónicos y procedimientos de cualquier tipo que se realicen y tramiten por el Ministerio Fiscal.

Disposición adicional décima. *Aplicación de la Ley en el ámbito de la jurisdicción militar.*

Las disposiciones contenidas en la presente Ley serán de aplicación en el ámbito de la jurisdicción militar, sin perjuicio de las especialidades propias de sus normas reguladoras.

Disposición adicional undécima. *Declaración de requerimientos tecnológicos de las reformas en las leyes procesales.*

Todo proyecto de ley que disponga o incluya reformas en las leyes procesales podrá ir acompañado de una declaración de requerimientos tecnológicos para su correcta implantación y aplicación.

Disposición adicional duodécima. *Relaciones de colaboración con los Colegios de Procuradores.*

Sin perjuicio de lo establecido en esta Ley y en especial de lo dispuesto en el Capítulo III de su Título IV, las relaciones de colaboración con los Colegios de Procuradores en el desempeño de las funciones que se les encomiendan para la organización de los servicios de notificaciones y traslados de copias previas para con estos profesionales de acuerdo con lo previsto en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y en la Ley de Enjuiciamiento Civil, podrán ser objeto del correspondiente y oportuno desarrollo en un convenio que se suscribirá con el Consejo General de Colegios de Procuradores de España, que recoja los presupuestos básicos de la presente Ley para la utilización de las tecnologías de la información en sus relaciones con la Administración de Justicia.

Disposición adicional decimotercera. *Publicaciones en el Tablón Edictal Judicial Único.*

Las publicaciones que, en cumplimiento de lo previsto en las leyes procesales, deban hacerse en el Tablón Edictal Judicial Único serán gratuitas en todo caso, sin que proceda contraprestación económica por parte de quienes la hayan solicitado.

Igualmente serán gratuitas las consultas en el tablón, así como las suscripciones que los ciudadanos puedan realizar en su sistema de alertas.

Disposición transitoria primera. *Coexistencia de procedimientos.*

1. Durante el tiempo en que coexistan procedimientos tramitados en soporte papel con procedimientos tramitados exclusivamente en formato electrónico, los servicios electrónicos de información del estado de la tramitación a que se refiere la presente Ley incluirán, respecto a los primeros, al menos la fase en la que se encuentra el procedimiento y el órgano o unidad responsable de su tramitación.

2. Los registros electrónicos existentes a la entrada en vigor de la presente Ley serán considerados registros judiciales electrónicos, regulándose por lo dispuesto en los artículos 30, 31 y 32 de esta Ley.

Disposición transitoria segunda. *Expediente electrónico con valor de copia simple.*

Si el estado de la técnica no hiciera posible remitir el expediente administrativo electrónico con los requisitos establecidos en su normativa específica, de conformidad con lo señalado en el apartado 4 del artículo 37 de esta Ley, dicho expediente tendrá el valor de copia simple. Será admisible la remisión del expediente en formato papel si las condiciones técnicas no permitiesen su remisión telemática.

Disposición transitoria tercera. *Tablón Edictal Judicial Único.*

La publicación de los edictos mediante el Tablón Edictal Judicial Único resultará de aplicación a partir del 1 de junio de 2021 tanto a los procedimientos que se inicien con posterioridad, como a los ya iniciados.

Disposición final primera. *Título competencial.*

La presente Ley se dicta al amparo de lo dispuesto en el artículo 149.1.5.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de Administración de Justicia.

Disposición final segunda. *Desarrollo normativo.*

Corresponde al Gobierno y a las Comunidades Autónomas, en el ámbito de sus respectivas competencias, dictar las disposiciones necesarias para el desarrollo y aplicación de la presente Ley.

Disposición final tercera. *Regulación del uso de los sistemas de videoconferencia en la Administración de Justicia.*

El Gobierno presentará un proyecto de ley que regule de manera integral el uso de los sistemas de videoconferencia en la Administración de Justicia.

Disposición final cuarta. *Entrada en vigor.*

La presente Ley entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

ANEXO

Definiciones

A efectos de la presente Ley, se entiende por:

– Actividad de servicio: Cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración.

– Actuación judicial automatizada: Actuación judicial producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular. Incluye la producción de actos de trámite o resolutorios de procedimientos, así como de meros actos de comunicación.

– Aplicación: Programa o conjunto de programas cuyo objeto es la resolución de un problema mediante el uso de la informática.

– Aplicación de fuentes abiertas: Aquella que se distribuye con una licencia que permite la libertad de ejecutarla, de conocer el código fuente, de modificarla o mejorarla y de redistribuir copias a otros usuarios.

– Autenticación: Acreditación por medios electrónicos de la identidad de una persona o ente, del contenido de la voluntad expresada en sus operaciones, transacciones y documentos y de la integridad y autoría de estos últimos.

– Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

– Canales: Estructuras o medios de difusión de los contenidos y servicios; incluyendo el canal presencial, el telefónico y el electrónico, así como otros que existan en la actualidad o puedan existir en el futuro (dispositivos móviles, TDT, etc.).

– Certificado electrónico: Según el artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

– Certificado electrónico reconocido: Según el artículo 11 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que preste.

– Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

– Disponibilidad: Propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

– Dirección electrónica: Identificador de un equipo o sistema electrónico desde el que se provee de información o servicios en una red de comunicaciones.

– Documento electrónico: Información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

– Espacios comunes o ventanillas únicas: Modos o canales (oficinas integradas, atención telefónica, páginas en Internet y otros) a los que los ciudadanos pueden dirigirse para acceder a las informaciones, trámites y servicios públicos determinados por acuerdo entre varias Administraciones.

– Estándar abierto: Aquel que reúna las siguientes condiciones:

Sea público y su utilización sea disponible de manera gratuita o a un coste que no suponga una dificultad de acceso,

su uso y aplicación no esté condicionado al pago de un derecho de propiedad intelectual o industrial.

– Firma electrónica: Según el apartado 1 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

– Firma electrónica avanzada: Según el apartado 2 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

– Firma electrónica reconocida: Según el apartado 3 del artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

– Índice electrónico: Relación de documentos electrónicos de un expediente electrónico, firmada por la Administración, órgano o entidad actuante, según proceda y cuya finalidad es garantizar la integridad del expediente electrónico y permitir su recuperación siempre que sea preciso.

– Infraestructuras y servicios comunes: Instrumentos operativos que facilitan el desarrollo y despliegue de nuevos servicios, así como la interoperabilidad de los existentes, creando escenarios de relación multilateral y que satisfacen las necesidades comunes en los distintos ámbitos administrativos; son ejemplos la Red de comunicaciones de las Administraciones públicas españolas, la Red transeuropea sTESTA y la plataforma de verificación de certificados electrónicos.

– Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

– Interoperabilidad: Capacidad de los sistemas de información, y por ende de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

– Interoperabilidad organizativa: Es aquella dimensión de la interoperabilidad relativa a la capacidad de las entidades y de los procesos a través de los cuales llevan a cabo sus actividades para colaborar con el objeto de alcanzar logros mutuamente acordados relativos a los servicios que prestan.

– Interoperabilidad semántico-jurídica: Es aquella dimensión de la interoperabilidad relativa a que la información, en el ámbito o de carácter judicial, intercambiada pueda ser interpretable de forma automática y reutilizable por aplicaciones que no intervinieron en su creación.

– Interoperabilidad técnica: Aquella dimensión de la interoperabilidad relativa a la relación entre sistemas y servicios de tecnologías de la información, incluyendo aspectos tales como las interfaces, la interconexión, la integración de datos y servicios, la presentación de la información, la accesibilidad y la seguridad, u otros de naturaleza análoga.

– Licencia pública de la Unión Europea («European Union Public Licence-EUPL»): Licencia adoptada oficialmente por la Comisión Europea en las veintitrés lenguas oficiales comunitarias para reforzar la interoperabilidad de carácter legal mediante un marco colectivo para la puesta en común de las aplicaciones del sector público.

– Medidas de seguridad: Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción o de recuperación.

– Medio electrónico: Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

– Metadato: Dato que define y describe otros datos. Existen diferentes tipos de metadatos según su aplicación.

– Metadato de gestión de documentos: Información estructurada o semiestructurada que hace posible la creación, gestión y uso de documentos a lo largo del tiempo en el contexto de su creación. Los metadatos de gestión de documentos sirven para identificar, autenticar y contextualizar documentos, y del mismo modo a las personas, los procesos y los sistemas que los crean, gestionan, mantienen y utilizan.

– Prestador de actividad de servicio: Cualquier persona física o jurídica que ofrezca o preste una actividad de servicio.

– Punto de acceso electrónico: Conjunto de páginas web agrupadas en un dominio de Internet cuyo objetivo es ofrecer al usuario, de forma fácil e integrada, el acceso a una serie de recursos y de servicios dirigidos a resolver necesidades específicas de un grupo de personas o el acceso a la información y servicios de una institución pública.

– Requisitos mínimos de seguridad: Exigencias necesarias para asegurar la información y los servicios.

– Sistema de firma electrónica: Conjunto de elementos intervinientes en la creación de una firma electrónica. En el caso de la firma electrónica basada en certificado electrónico, componen el sistema, al menos, el certificado electrónico, el soporte, el lector, la aplicación de firma utilizada y el sistema de interpretación y verificación utilizado por el receptor del documento firmado.

– Sellado de tiempo: Acreditación a cargo de un tercero de confianza de la fecha y hora de realización de cualquier operación o transacción por medios electrónicos.

– Sello de tiempo: La asignación por medios electrónicos de una fecha y hora a un documento electrónico con la intervención de un prestador de servicios de certificación que asegure la exactitud e integridad de la marca de tiempo del documento.

– Sistema de información: Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

– Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

§ 66

Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité técnico estatal de la Administración judicial electrónica

Ministerio de Justicia
«BOE» núm. 146, de 19 de junio de 2013
Última modificación: sin modificaciones
Referencia: BOE-A-2013-6657

El proceso de modernización de la Administración de Justicia es el resultado de una larga evolución histórica de la que pueden destacarse diversos hitos de relevancia: por una parte, el Pacto de Estado para la Reforma de la Justicia de 2001, la Carta de Derechos de los Ciudadanos ante la Justicia aprobada como Proposición no de Ley el 22 de abril de 2002 y el Plan de Transparencia Judicial aprobado por Consejo de Ministros de 21 de octubre de 2005; y, por otra, diversos instrumentos legales y convencionales como la reforma operada por la Ley Orgánica 16/1994, de 8 de noviembre, por la que se reforma la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, así como el Convenio para el establecimiento del Esquema judicial de interoperabilidad y seguridad en el ámbito de la Administración de Justicia celebrado el 30 de septiembre de 2009, entre el Ministerio de Justicia, el Consejo General del Poder Judicial y la Fiscalía General del Estado, al que, posteriormente, se adhirieron, en fecha 10 de diciembre de 2009, las Comunidades Autónomas con competencias en materia de justicia.

La Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, supone la aspiración de instaurar plena y eficazmente la Administración judicial electrónica, siendo uno de sus pilares básicos el uso generalizado y obligatorio de las referidas tecnologías, tanto por los órganos judiciales como por los profesionales y ciudadanos que se relacionan con aquellos, regulando, a tal fin, entre otras cuestiones, los requisitos mínimos necesarios de interoperabilidad y seguridad que, posteriormente, deberán, dice la citada norma, ser desarrollados por el Esquema judicial de interoperabilidad y seguridad, que permitirá el cumplimiento de los objetivos marcados por dicha Ley.

La Ley 18/2011, de 5 de julio, sienta las bases del presente desarrollo normativo además de consolidar en una norma legal el marco de colaboración y cooperación entre las Administraciones con competencias en materia de Justicia contenidas en los citados Convenios de colaboración.

Para conseguir todo ello, tanto en su preámbulo como en su articulado, se prevé la necesidad de acometer un desarrollo normativo que se torna imprescindible para la efectiva implantación de la Administración judicial electrónica. Entre otros, en lo que ahora se refiere, establece, en su preámbulo, la regulación y creación de un órgano que fije las pautas necesarias para asegurar la interoperabilidad de los sistemas y aplicaciones de la Administración de Justicia y la cooperación entre las distintas administraciones. Tras ello, en su Título V, regula la cooperación entre las Administraciones con competencias en materia

de Justicia, estableciendo los aspectos básicos sobre los que debe asentarse la necesaria cooperación y colegiación de esfuerzos entre las Administraciones con competencias en materia de justicia y constituyendo el Comité técnico estatal de la Administración judicial electrónica, con importantes competencias en orden a favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados en la Administración de Justicia, así como para asegurar la cooperación entre las distintas Administraciones, siendo su función principal, conforme al art. 44 y siguientes de la Ley 18/2011, de 5 de julio, la de establecer las bases que permitan el desarrollo de dicho Esquema judicial de interoperabilidad y seguridad.

En especial, la Disposición adicional primera de la Ley 18/2011, de 5 de julio, dispone que «la estructura, composición y funciones del Comité técnico estatal de la Administración judicial electrónica serán establecidas reglamentariamente por el Gobierno, mediante real decreto, previo informe del Consejo General del Poder Judicial, de la Fiscalía General del Estado, de la Agencia Española de Protección de Datos y de las Comunidades Autónomas con competencias en la materia».

El Comité técnico estatal de la Administración judicial electrónica, como órgano de cooperación, surge con la vocación de coordinación y planificación conjunta en el ámbito de las nuevas tecnologías aplicadas a la Administración de Justicia para evitar duplicidad de esfuerzos en este ámbito, coherentemente con el principio de eficiencia en la asignación y utilización de los recursos públicos previsto en el artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.

En consecuencia, el Comité técnico estatal de la Administración judicial electrónica que se regula en el presente real decreto, cuya constitución está alineada con la estrategia de racionalización de estructuras, procedimientos y recursos del programa de reformas del Gobierno, plasmada en la creación de la Comisión para la Reforma de las Administraciones Públicas, a la que ofrecerá la información precisa sobre sus actuaciones, se configura como una de las piezas esenciales para la consecución de los objetivos establecidos en la Ley 18/2011, de 5 de julio, en orden a la interoperabilidad de las distintas aplicaciones que se utilizan en la Administración de Justicia de modo que, en este contexto, dicho órgano ostentará la dirección, coordinación, impulso y competencias para desarrollar el Esquema judicial de interoperabilidad y seguridad.

La regulación del Comité técnico estatal de la Administración judicial electrónica que contiene el presente real decreto se realiza bajo dos perspectivas compatibles. Por una parte, atiende a las expresas previsiones contempladas en la Ley 18/2011, de 5 de julio, al respecto de la arquitectura normativa de la Administración judicial electrónica y, por otra, dicha regulación dota de un sistema determinado y concreto pero a su vez flexible que permita que, en un futuro, el Comité técnico estatal de la Administración judicial electrónica, conforme evolucione su actividad y el estado tecnológico y jurídico de la Administración judicial electrónica, pueda acometer cuantas acciones se estimen oportunas de acuerdo con lo previsto en el artículo 44.2 de la Ley 18/2011, de 5 de julio.

El presente real decreto tiene carácter organizativo a fin de recoger estrictamente las antedichas cuestiones necesitadas de desarrollo. Así, se estructura en 3 capítulos comprensivos de 20 artículos. El capítulo I contiene las disposiciones generales comunes a todo el Comité técnico estatal de la Administración judicial electrónica ahora regulado. El capítulo II dedicado a las competencias, composición y funciones del Comité técnico estatal de la Administración judicial electrónica y el capítulo III dividido en cinco secciones desarrolla la organización y funcionamiento de los órganos de Comité técnico estatal de la Administración judicial electrónica, bajo la citada doble perspectiva de establecer los órganos del mismo que posibiliten una efectiva constitución y funcionamiento y a la vez evitando incurrir en una regulación rígida que impida la evolución de dicho órgano, de modo que, con carácter general, se prevé el Pleno, la Comisión Permanente, el Presidente y la Secretaría General del Comité técnico estatal de la Administración judicial electrónica como órganos necesarios del mismo sin perjuicio de la posibilidad de constituir otros órganos, oficinas o grupos de trabajo que asesoren y sirvan de soporte, de modo duradero o transitorio, al Comité técnico estatal de la Administración judicial electrónica para el ejercicio de sus competencias. Por último, el real decreto contiene 7 disposiciones adicionales, 2 disposiciones transitorias y 2 disposiciones finales dirigidas en general, a garantizar la

participación de otras Instituciones o Administraciones así como determinadas previsiones de futuro como la continuidad de las actividades y normativa hasta ahora desarrolladas en el seno de los referidos Convenios de colaboración y adhesión, por cuanto que, de no darse la misma, podrían frustrarse las iniciativas que, en materia de Administración judicial electrónica, han ejecutado el Consejo General del Poder Judicial, el Ministerio de Justicia, la Fiscalía General del Estado y las comunidades autónomas con competencias en la materia; así como la correspondiente previsión competencial y de entrada en vigor.

Este real decreto ha sido informado por el Consejo General del Poder Judicial, el Consejo Fiscal, la Agencia Española de Protección de Datos y las comunidades autónomas con competencias en materia de justicia.

En su virtud, a propuesta del Ministro de Justicia, con la aprobación previa del Ministro de Hacienda y Administraciones Públicas, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 7 de junio de 2013,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

El objeto de este real decreto es la regulación de la estructura, composición y funciones del Comité técnico estatal de la Administración judicial electrónica creado por la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Artículo 2. *Ámbito de aplicación.*

El presente real decreto será de aplicación a la Administración de Justicia, para favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados, en las relaciones de los ciudadanos y profesionales que actúen en su ámbito, así como a las relaciones entre aquélla y el resto de Administraciones y organismos públicos.

Artículo 3. *Naturaleza.*

El Comité técnico estatal de la Administración judicial electrónica es el órgano de cooperación en materia de Administración judicial electrónica, sin perjuicio de las competencias del Consejo General del Poder Judicial como garante de la compatibilidad de los sistemas informáticos prevista en el artículo 230.5 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. Dicho Comité actuará con plena autonomía en el ejercicio de sus funciones.

Artículo 4. *Principios.*

El Comité técnico estatal de la Administración judicial electrónica ejercerá sus funciones en el ámbito de sus competencias bajo los siguientes principios:

a) Colegiación de esfuerzos.
b) Cooperación interadministrativa.
c) Reutilización de la información y tecnología.
d) Fomento, difusión y empleo de los medios electrónicos en sus relaciones internas y externas garantizando que sean accesibles para las personas con discapacidad.
e) Transparencia.
f) Neutralidad jurídica, tecnológica y política.

Artículo 5. *Régimen jurídico.*

En lo no previsto en la Ley 18/2011, de 5 de julio, el régimen jurídico y la actuación del Comité técnico estatal de la Administración judicial electrónica, como órgano de cooperación

en materia de Administración judicial electrónica, se regirá por lo dispuesto en la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus propias normas de funcionamiento interno que, con respeto al anterior marco normativo, aprobará de conformidad con lo dispuesto en el presente real decreto.

CAPÍTULO II

Competencias, composición y funciones del Comité técnico estatal de la Administración judicial electrónica

Artículo 6. *Competencias.*

Son competencias del Comité técnico estatal de la Administración Judicial electrónica:

a) Favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados por la Administración de Justicia.

b) Preparar planes y programas conjuntos de actuación para impulsar el desarrollo de la Administración judicial electrónica, respetando, en todo caso, las distintas competencias atinentes a los medios materiales de la Administración de Justicia.

c) Promover la cooperación de otras Administraciones Públicas con la Administración de Justicia para suministrar a los órganos judiciales, a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, la información que precisen en el curso de un proceso judicial en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y en las leyes procesales.

d) Fijar las bases para el desarrollo del Esquema judicial de interoperabilidad y seguridad de modo que permita, a través de las plataformas tecnológicas necesarias, la interoperabilidad total de todas las aplicaciones informáticas al servicio de la Administración de Justicia.

e) Elaborar y difundir las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones.

f) Actualizar permanentemente el Esquema judicial de interoperabilidad y seguridad de conformidad con las necesidades derivadas de la evolución jurídica y tecnológica en la materia, desarrollando, a tal fin, las guías y normas técnicas de aplicación.

g) Las resoluciones por las que se adopten dichas bases, guías de interoperabilidad y seguridad judicial así como las guías y normas técnicas de aplicación, deberán publicarse íntegramente en el Boletín Oficial del Estado y en los diarios oficiales de las Comunidades Autónomas con competencias asumidas en materia de justicia, produciéndose, en todo caso, su entrada en vigor, salvo expresa previsión en otro sentido, desde su completa publicación en el Boletín Oficial del Estado.

h) Velar por el establecimiento de los mecanismos de control para asegurar, de forma efectiva, el cumplimiento del Esquema judicial de interoperabilidad y seguridad.

i) Adoptar los acuerdos necesarios para que, en la creación y gestión del punto de acceso general de la Administración de Justicia por el Ministerio de Justicia, se asegure la completa y exacta incorporación de la información que preste dicho punto de acceso general.

j) Determinar las condiciones y garantías de las comunicaciones en el seno de la Administración de Justicia estableciendo la relación de emisores y receptores autorizados y la naturaleza de los datos a intercambiar.

k) Realizar el correspondiente análisis de rediseño funcional de los procedimientos, procesos y servicios, a cuya gestión se apliquen los medios electrónicos.

l) Establecer, para los supuestos de la actuación judicial automatizada, la definición de las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, la auditoría del sistema de información y de su código fuente, incluidos los indicadores de gestión, sin perjuicio, en este último supuesto de aquellos indicadores que fueren señalados por la Comisión Nacional de Estadística Judicial en el ámbito de sus

competencias, así como los necesarios para cumplir con la planificación estadística recogida en el Plan Estadístico Nacional.

m) Constituir, dirigir y coordinar la actividad de los grupos de trabajo necesarios para la redacción y mantenimiento de guías y normas técnicas de aplicación o para el desarrollo de otras de sus competencias.

n) Informar, cuando así le sea solicitado, sobre los requerimientos tecnológicos de aquellas normas que sean de aplicación o incidan en la Administración de Justicia.

o) Informar con carácter preceptivo sobre las normas y convenios que se refieran a la interoperabilidad y seguridad de la Administración judicial electrónica.

p) Emitir, en su caso, informes, generales o especiales, sobre cualquier iniciativa o norma técnica relativa a la Administración judicial electrónica, así como a los sistemas o aplicaciones relacionados con la misma.

q) Aquellas otras que legalmente se determinen.

r) Promover que los medios electrónicos de la Administración de Justicia en sus relaciones internas y externas sean accesibles para las personas con discapacidad.

Artículo 7. *Composición.*

Estarán representados en el Comité técnico estatal de la Administración judicial electrónica:

a) El Consejo General del Poder Judicial.

b) El Ministerio de Justicia.

c) La Fiscalía General del Estado.

d) Las Comunidades Autónomas con competencias en materia de Administración de Justicia.

Artículo 8. *Función consultiva.*

1. El Comité técnico estatal de la Administración judicial electrónica es el órgano consultivo e impulsor de la cooperación en materia de Administración judicial electrónica.

2. El Comité técnico estatal de la Administración judicial electrónica deberá informar sobre cualquier proyecto normativo que incida sobre la interoperabilidad y/o seguridad de la Administración judicial electrónica.

3. El Comité técnico estatal de la Administración judicial electrónica dictará las normas de funcionamiento interno reguladoras de los procedimientos a seguir en la tramitación y adopción de acuerdos propios del ejercicio de tal función.

4. Sin perjuicio de lo dispuesto en las referidas normas de funcionamiento interno, el Comité técnico estatal de la Administración judicial electrónica emitirá dichos informes con carácter ordinario, en cuyo caso dispondrá de un plazo de tres meses, o con carácter urgente, en el plazo de un mes a contar, en ambos casos, desde que la petición tenga entrada en el Comité técnico estatal de la Administración judicial electrónica.

En dichas normas, podrá establecer los diversos canales informativos atendiendo al sujeto, objeto y naturaleza de la consulta planteada al Comité técnico estatal de la Administración judicial electrónica.

Tal normativa, deberá contemplar, al menos, el dictado de informes o dictámenes en el ejercicio de la preceptiva función consultiva así como de circulares, instrucciones o recomendaciones según el caso.

5. Las funciones anteriormente indicadas lo serán sin perjuicio de la competencia prevista en el artículo 230.5 de la Ley Orgánica 6/1985, de 1 de julio, respecto a la compatibilidad de los sistemas informáticos de gestión procesal.

CAPITULO III

Organización y funcionamiento

Sección 1.ª Órganos

Artículo 9. *Estructura.*

Son órganos necesarios del Comité técnico estatal de la Administración judicial electrónica el Pleno, la Comisión Permanente, el Presidente y la Secretaría General.

El Comité técnico estatal de la Administración judicial electrónica, de acuerdo a sus normas de funcionamiento interno, podrá disponer de otros órganos o grupos de apoyo, pudiendo ser desempeñadas funciones de asesoría, consultoría y/o soporte al Comité, o a sus órganos, por aquellos órganos, oficinas o grupos de trabajo que el Pleno considere oportuno constituir en su seno.

Artículo 10. *Régimen de funcionamiento.*

1. El Comité técnico estatal de la Administración judicial electrónica actuará en Pleno, Comisión Permanente y, en su caso, mediante grupos de trabajo, pudiendo, a su vez, realizar internamente delegación de funciones o crear aquellos órganos dependientes de los mismos que considere preciso para el óptimo desempeño de sus funciones. Estará asistido por una oficina técnica para el desempeño de las funciones que se le encomienden, provista de los medios personales y materiales que cada uno de sus órganos e instituciones aporte, sin que ello suponga incremento del gasto público.

2. El funcionamiento de los diversos órganos del Comité se regirá por lo dispuesto en este Real Decreto y en las normas de funcionamiento interno previstas en el mismo.

3. El Pleno aprobará, por mayoría absoluta de sus miembros, las normas de funcionamiento interno que se consideren oportunas para el mejor cumplimiento de las funciones encomendadas al Comité técnico estatal de la Administración judicial electrónica. La propuesta de las citadas normas corresponderá a la Comisión Permanente sin perjuicio de la delegación del ejercicio de las competencias que en su caso se acordaren. Al menos la normativa reguladora del Pleno y la Comisión Permanente, así como los acuerdos adoptados por el Pleno, se publicarán en la sede electrónica del Comité técnico estatal de la Administración judicial electrónica. El Comité técnico estatal de la Administración judicial electrónica, en sus normas de funcionamiento interno, podrá, respetando la anterior publicidad, establecer otros supuestos o medios de publicación de sus actuaciones o normas propias.

4. Para la válida celebración de sesiones y toma de acuerdos del Pleno y de la Comisión Permanente se requerirá la presencia del Presidente, del Secretario General y la mitad, al menos, del resto de sus miembros.

La convocatoria de las sesiones ordinarias y extraordinarias, así como el orden del día deberá enviarse con la suficiente antelación a los distintos vocales por medio telemático que ofrezca garantía de recepción, junto con la documentación que se considere necesaria.

De las reuniones que se celebren por los órganos de Comité técnico estatal de la Administración judicial electrónica se levantará acta por el Secretario General del mismo.

5. Para la válida adopción de los acuerdos del Pleno y de la Comisión Permanente, será preciso el voto favorable de la mayoría absoluta de los asistentes de dichos órganos, excepto para la elaboración de informes consultivos en que será suficiente su aprobación por mayoría simple de los asistentes.

Los acuerdos que se alcancen en el seno del Comité técnico estatal de la Administración judicial electrónica se adoptarán garantizando la previa búsqueda del consenso entre sus miembros. En aquellos casos en que no sea posible tal consenso, deberá reformularse la propuesta sometida a votación. De no lograrse por tal medio el acuerdo, a través de las normas de funcionamiento interno se establecerá el modo de someter el asunto debatido al régimen de mayorías cualificadas o simples, dirimir empates y el voto de calidad del Presidente.

6. El funcionamiento interno del Comité técnico estatal de la Administración judicial electrónica, o de sus órganos, será, en todo caso electrónico, sin perjuicio de los supuestos

de fuerza mayor o imposibilidad jurídica o técnica apreciada por el Pleno. Deberá fomentar el uso de las tecnologías de la información y comunicación y el procedimiento electrónico en su relación con ciudadanos y Administraciones en el ámbito de la Administración de Justicia.

Sección 2.ª Del pleno

Artículo 11. *Composición.*

El Pleno del Comité técnico estatal de la Administración judicial electrónica estará integrado por los siguientes miembros:

a) El Presidente del Comité técnico estatal de la Administración judicial electrónica, que será el Secretario de Estado de Justicia y un Vocal del Consejo General del Poder Judicial conforme al turno rotatorio previsto en el artículo 16, los cuales serán vocales cuando no ejerzan la Presidencia.

b) Vocales. El Pleno del Comité técnico estatal de la Administración judicial electrónica estará además integrado por:

1. Un vocal en representación de la Fiscalía General del Estado, que corresponderá al Fiscal Jefe de la Unidad de Apoyo.

2. Un vocal en representación de cada una de las Comunidades Autónomas con competencias en esta materia, designado por éstas, con rango de Consejero de su órgano de gobierno o, en su defecto, no inferior a Director General.

c) Secretario, con voz pero sin voto, siendo desempeñadas sus funciones por quien desempeñare la Secretaría General del Comité técnico estatal de la Administración judicial electrónica.

Artículo 12. *Competencias.*

1. Son competencias del Pleno:

a) Impulsar la colaboración y cooperación para favorecer la compatibilidad y asegurar la interoperabilidad de los sistemas y aplicaciones empleados por la Administración de Justicia, fijando estrategias y estableciendo planes conjuntos de actuación para impulsar el desarrollo de la Administración judicial electrónica, respetando en todo caso las distintas competencias atinentes a los medios materiales de la Administración de Justicia.

b) Aprobar las bases para la actualización permanente del Esquema judicial de interoperabilidad y seguridad, en paralelo al progreso de los servicios de Administración judicial electrónica, de la evolución tecnológica y a medida que vayan consolidándose las infraestructuras que le apoyan.

c) Aprobar y elevar al Ministerio de Justicia los acuerdos necesarios para la creación y gestión del punto de acceso general de la Administración de Justicia.

d) Promover la cooperación de otras Administraciones Públicas con la Administración de Justicia para suministrar a los órganos judiciales, a través de las plataformas de interoperabilidad establecidas por el Consejo General del Poder Judicial y por las Administraciones competentes en materia de Administración de Justicia, la información que precisen en el curso de un proceso judicial. El Pleno del Comité técnico estatal de la Administración judicial electrónica mantendrá las oportunas relaciones con los órganos de cooperación entre las distintas Administraciones que se creen a tal efecto.

e) Aprobar el calendario de sesiones ordinarias del Pleno, Comisión Permanente u otros órganos, propuesto por la Presidencia del Comité técnico estatal de la Administración judicial electrónica.

f) Establecer los planes e informes a elaborar para el conocimiento y seguimiento periódicos del estado de la interoperabilidad, seguridad y grado de implantación de la Administración judicial electrónica. Aprobar los mismos y autorizar su difusión pública.

g) Velar por el establecimiento de los mecanismos de control para asegurar, de forma efectiva, el cumplimiento del Esquema judicial de interoperabilidad y seguridad.

2. El Pleno del Comité técnico estatal de la Administración judicial electrónica elevará anualmente al Consejo de Ministros y al Consejo General del Poder Judicial un informe en el

que se recogerá el grado de avance en la implantación de la Administración judicial electrónica.

Artículo 13. *Funcionamiento.*

1. El Pleno se reunirá en sesiones ordinarias, que se celebrarán, al menos, dos veces al año, o extraordinarias. El régimen de convocatoria, constitución, debate y modo de adopción de acuerdos será desarrollado en sus normas de funcionamiento interno, sin perjuicio de lo regulado en el presente Real Decreto.

Las reuniones se anunciarán con suficiente antelación de modo que los miembros tengan la posibilidad de incorporar nuevos puntos en el orden del día. En los intervalos entre reuniones se mantendrá abierto un buzón en el que los integrantes del Comité técnico estatal de la Administración judicial electrónica puedan remitir los informes, consultas y sugerencias que consideren oportunas. Se fomentará en las reuniones y grupos de trabajo el empleo de las nuevas tecnologías de la comunicación.

2. Las sesiones ordinarias serán convocadas por la Presidencia con, al menos, periodicidad semestral y con los requisitos sobre antelación y orden del día previstos en las normas de funcionamiento interno que apruebe el Pleno. El régimen de votos deberá respetar la debida paridad entre los miembros del Comité técnico estatal de la Administración judicial electrónica con independencia del número de representantes miembros o asistentes por cada Institución o Administración integrante del mismo.

3. Las sesiones extraordinarias serán convocadas por la Presidencia del Comité técnico estatal de la Administración judicial electrónica cuando así lo considere necesario o, a solicitud, sucintamente motivada, de una cuarta parte de los miembros del Pleno, en el plazo de dos días desde que dicha convocatoria fuera presentada en la Secretaría Permanente del Comité técnico estatal de la Administración judicial electrónica.

Sección 3.ª De la comisión permanente

Artículo 14. *Composición.*

1. La Comisión Permanente del Comité técnico estatal de la Administración judicial electrónica estará compuesta por los siguientes miembros:

a) Presidente: el Secretario General de la Administración de Justicia y un Vocal del Consejo General del Poder Judicial en turno rotatorio por periodos bienales, los cuales serán vocales cuando no ejerzan la Presidencia de la Comisión Permanente. El Pleno podrá prorrogar dicho mandato en atención a las actividades o necesidades del Comité técnico estatal de la Administración judicial electrónica. Las normas de funcionamiento interno del Comité técnico estatal de la Administración judicial electrónica determinarán el régimen de funcionamiento, vacancias y ausencias del Presidente de dicha Comisión.

b) Vocales: la Comisión Permanente del Comité técnico estatal de la Administración judicial electrónica estará además integrada por:

1.º Un vocal en representación de la Fiscalía General del Estado, que corresponderá a un Fiscal de la Unidad de Apoyo.

2.º Un vocal en representación de las comunidades autónomas con competencias en materia de justicia, que se designará anualmente por las mismas, el cual deberá informar con suficiente antelación a las comunidades sobre los asuntos tratados.

Cuando se hubieren tratado estos asuntos que pudieren afectar particularmente a una o varias comunidades autónomas, y previa petición de convocatoria a la siguiente sesión, las mismas podrán designar un representante, con voz pero sin voto, por cada una de ellas.

3.º Un vocal representando al Cuerpo de Secretarios Judiciales con conocimientos en materia de Administración judicial electrónica, designado por el Pleno.

4.º Hasta un máximo de 5 vocales con perfil y formación técnica en materia de Administración judicial electrónica, designados por el Pleno.

c) Secretario, con voz pero sin voto, siendo desempeñadas sus funciones por el titular de la Secretaría General del Comité técnico estatal de la Administración judicial electrónica o

por quien, en los supuestos recogidos en las normas de funcionamiento interno, le sustituyere en su caso.

2. La presidencia de la Comisión Permanente podrá invitar a incorporarse, con voz pero sin voto, a representantes de otras instituciones, Administraciones, corporaciones o personas públicas o privadas. Dicha iniciativa podrá ejercerse de oficio o a instancia del resto de miembros del Pleno en los términos que se establezcan reglamentariamente.

3. Las reuniones de la Comisión Permanente se celebrarán, al menos, cada tres meses rigiendo, para las demás cuestiones relativas a su funcionamiento, lo dispuesto en el artículo 13 del presente Real Decreto.

Artículo 15. *Competencias.*

Son competencias de la Comisión Permanente:

a) Preparar propuestas de planes estratégicos y programas conjuntos de actuación para impulsar el desarrollo de la Administración judicial electrónica, y su elevación para su aprobación por el Pleno.

b) Elaborar y elevar al Pleno para su aprobación las bases para la actualización del Esquema judicial de interoperabilidad y seguridad.

c) Realizar los análisis y trabajos técnicos que sirvan de base para la toma de decisiones por el Pleno en el ámbito de la interoperabilidad.

d) Dar seguimiento a la ejecución de los programas conjuntos de actuación, así como elevar informe al Pleno sobre factores que puedan incidir en su ejecución.

e) Elaborar y elevar al Pleno las propuestas de actuación cuya aprobación le correspondan a éste así como proponer cuantos estudios, proyectos e iniciativas en materia de interoperabilidad judicial considere adecuadas.

f) Elaborar y elevar al Pleno los acuerdos oportunos para asegurar la completa y exacta incorporación de la información y accesos publicados en el punto de acceso general de la Administración de Justicia.

g) Proponer las condiciones y garantías por las que se regirá el intercambio electrónico de datos en entornos cerrados de comunicación.

h) Elaborar la propuesta de los análisis de rediseño funcional y simplificación en la aplicación de medios electrónicos a la gestión de los procedimientos, procesos o servicios.

i) Constituir los grupos de trabajo que consideren necesarios para el desarrollo de sus funciones.

j) En los casos de actuación judicial automatizada, proponer:

1. Las especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso la auditoría del sistema de información y de su código fuente.

2. En el ámbito de las competencias del Comité técnico estatal de la Administración judicial electrónica, las recomendaciones sobre indicadores de gestión que deberán incluir los sistemas.

k) Identificar y catalogar los servicios de interoperabilidad que prestaren las Administraciones Públicas y los órganos de la Administración de Justicia.

l) Elaborar, desarrollar, mantener y elevar, para su aprobación y difusión, las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones, guías y normas técnicas de aplicación, guía técnica de seguridad y cuantas otras normativas sean precisas establecer en el ejercicio de sus competencias, sin perjuicio de lo establecido en el artículo 230.5 de la Ley Orgánica 6/1985, de 1 de julio.

m) Constituir, dirigir y coordinar la actividad de los grupos de trabajo necesarios para la redacción y mantenimiento de guías y normas técnicas de aplicación o para el desarrollo de otras de sus competencias.

n) Proponer al Pleno los planes e informes, generales o sectoriales, y criterios para su análisis y elaboración, que permitan el conocimiento y seguimiento periódicos del estado de la interoperabilidad y seguridad judicial y grado de implantación de la Administración judicial electrónica.

o) Ejecutar los planes e informes que establezca el Comité técnico estatal de la Administración judicial electrónica para el conocimiento y seguimiento periódicos del estado

de la interoperabilidad y seguridad judicial y grado de implantación de la Administración judicial electrónica.

p) Disponer de la relación consolidada y actualizada de las aplicaciones informáticas al servicio de la Administración de Justicia a fin de que el Ministerio de Justicia y las restantes Administraciones competentes dispongan de información de valor para el mantenimiento del Directorio General de información tecnológica judicial.

q) Celebrar otras actividades para el intercambio de experiencias y proyectos en estas materias.

r) Ejecutar los acuerdos adoptados y ejercer cualesquiera otras competencias que le sean delegadas por el Pleno o atribuidas normativamente.

Sección 4.ª Del presidente

Artículo 16. *Presidente.*

El Comité técnico estatal de la Administración judicial electrónica estará copresidido por un representante del Consejo General del Poder Judicial y otro del Ministerio de Justicia, por períodos bienales conforme a un turno rotatorio.

La Presidencia del Comité técnico estatal de la Administración judicial electrónica será ejercida, en su turno correspondiente, por el Secretario de Estado de Justicia y por un Vocal del Consejo General del Poder Judicial.

Artículo 17. *Funciones.*

El Presidente del Comité técnico estatal de la Administración judicial electrónica tendrá las siguientes funciones:

a) Ostentar la máxima representación e interlocución del Comité técnico estatal de la Administración judicial electrónica.

b) Convocar, dirigir y ordenar las sesiones del Pleno, en los términos fijados en el presente real decreto y demás normativa aplicable.

c) Invitar a incorporarse, con voz pero sin voto, a aquellas personas, físicas o jurídicas, públicas o privadas, que, por su experiencia, conocimiento o dedicación en el ámbito judicial o electrónico, aporten un beneficio para la obtención de las finalidades propias del Comité técnico estatal de la Administración judicial electrónica.

Dichas personas podrán serlo a título particular o como representantes de aquellas Instituciones, Administraciones, entidades, o grupos de trabajo instaurados en las mismas, por su condición de profesionales de reconocido prestigio en aquella materia o por ser referencia en la misma como observatorios, sedes, foros u órganos de debate.

Dicho ofrecimiento podrá darse a su instancia o a la de los miembros del Comité técnico estatal de la Administración judicial electrónica siendo tal participación regulada en las normas de funcionamiento interno que éste establezca donde, en todo caso, deberá indicarse si dicha participación lo es en grupos de trabajo, en condición de Observadores o mediante cualesquiera otras fórmulas que permitan la difusión mutua de conocimiento y experiencias en el ámbito de actuación del Comité técnico estatal de la Administración judicial electrónica. De igual manera, se regulará el modo en que el Comité técnico estatal de la Administración judicial electrónica o sus órganos puedan participar en otros observatorios, sedes, foros u órganos a los que fuere invitado o solicitada su participación.

En todo caso, a los efectos de tal participación externa, el Comité técnico estatal de la Administración judicial electrónica deberá prestar especial atención a los grupos de trabajo de aquellas Administraciones Públicas u organismos nacionales y de la Unión Europea que, por su objeto y experiencia, desempeñan una especial actividad en las materias comunes objeto del Comité técnico estatal de la Administración judicial electrónica.

d) Aquellas otras que legal o internamente le sean conferidas.

Sección 5.ª De la secretaría general

Artículo 18. *Secretaría General.*

La Secretaría General del Comité técnico estatal de la Administración judicial electrónica lo será, indistintamente, del Pleno y de la Comisión Permanente, todo ello, sin perjuicio del resto de las atribuciones que le sean propias y de la potestad de delegación y sustitución que puedan establecerse en las normas de funcionamiento.

Artículo 19. *Estructura y organización.*

1. La persona titular de la Secretaría General tendrá la condición de Secretario General del Comité técnico estatal de la Administración judicial electrónica. El Pleno podrá, a la luz de las necesidades del Comité técnico estatal de la Administración judicial electrónica o de sus órganos, dotar de estructura y medios propios a la Secretaría General, que se realizará con los medios personales y materiales actualmente existentes, así como establecer una Secretaría para cada órgano del Comité técnico estatal de la Administración judicial electrónica que, en todo caso, dependerán de la Secretaría General.

2. La Secretaría General recaerá en un miembro de las Carreras Judicial o Fiscal, o perteneciente al Cuerpo de Secretarios Judiciales o a alguno de los Cuerpos del subgrupo A1 a que se refiere el artículo 76 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público en los que se hubiere ingresado por razón de su titulación como licenciado en Derecho, y que se encuentre destinado en el Consejo General del Poder Judicial o en el Ministerio de Justicia. El Secretario General será designado y cesado, en su caso, por el Pleno del Comité técnico estatal de la Administración judicial electrónica. La designación lo será por un periodo de 4 años, y el cese por las causas legalmente establecidas y a regular en las normas de funcionamiento interno.

3. El Pleno del Comité técnico estatal de la Administración judicial electrónica, a la vista de las necesidades del mismo o de sus órganos, podrá acordar que la Secretaría General del Comité recaiga de modo continuo en alguna de las Administraciones o Instituciones miembros del citado Comité, adoptando o elevando en tal supuesto al órgano competente los acuerdos de índole jurídica o presupuestaria que consideren pertinentes.

4. Para el desempeño de las funciones de la Secretaría General o de las dependientes de la misma, podrán adscribirse medios humanos y materiales propios o ajenos a la Administración que designó la persona nombrada Presidente.

5. En cualquier caso, la Secretaría General deberá garantizar el empleo de medios electrónicos en su funcionamiento y relación con Administraciones, Instituciones o ciudadanos.

Artículo 20. *Funciones.*

La Secretaría del Comité técnico estatal de la Administración judicial electrónica ejercerá las siguientes funciones:

a) La tramitación de los asuntos propios del Comité técnico estatal de la Administración judicial electrónica o sus órganos y el seguimiento de sus actividades.

b) La formación y tramitación de los procedimientos y la propuesta o, en su caso, adopción de los acuerdos objeto de su competencia.

c) El archivo, custodia y notificación de los actos acordados por el Comité técnico estatal de la Administración judicial electrónica o sus órganos.

d) La interlocución con otras Administraciones, Instituciones o ciudadanos.

e) La preparación de las sesiones y acuerdos a adoptar por el Comité técnico estatal de la Administración judicial electrónica o sus órganos.

f) La ejecución de aquellos acuerdos adoptados por el Comité técnico estatal de la Administración judicial electrónica o sus órganos.

g) Aquellas otras legal o internamente atribuidas.

Disposición adicional primera. *Efectos económicos.*

La aprobación del presente real decreto y las previsiones recogidas en el mismo no supondrán en ningún caso incremento del gasto público ni de dotaciones de personal, ni de retribuciones ni de créditos.

A fin de poder acometer, de conformidad con dicho principio, las actuaciones encomendadas al Comité técnico estatal de la Administración judicial electrónica, sus miembros contribuirán con los medios propios de los que ya dispongan para un continuo y estable desempeño de sus competencias de acuerdo a los principios de reutilización y cooperación entre Administraciones.

Los diversos convenios de carácter trilateral que se suscriban en el ámbito del Comité técnico estatal de la Administración judicial electrónica, darán participación a este órgano sin que ello suponga un coste para el mismo.

Disposición adicional segunda. *Incorporación de nuevos miembros.*

Desde el momento en que sea efectivo un traspaso de competencias en esta materia a una comunidad autónoma, ésta será miembro de pleno derecho del Comité técnico estatal de Administración judicial electrónica. En tal supuesto, el Presidente del Comité técnico estatal de la Administración judicial electrónica dará traslado a la nueva Administración de las actividades y convocatorias de sesiones pendientes de celebración.

Disposición adicional tercera. *Constitución del Comité técnico estatal de la Administración judicial electrónica.*

En el plazo de tres meses, a contar desde la entrada en vigor del presente real decreto, la institución en quien recaigan las funciones de Secretaría Permanente derivadas del Convenio de Colaboración entre el Ministerio de Justicia, el Consejo General del Poder Judicial y la Fiscalía General del Estado para el establecimiento del Esquema judicial de interoperabilidad y seguridad en el ámbito de la Administración de Justicia, procederá a convocar la primera sesión del Comité técnico estatal de la Administración judicial electrónica, que tendrá carácter constitutivo del mismo. Podrán, asimismo, adoptarse aquellos acuerdos necesarios para el inicio de sus actividades y funcionamiento.

Disposición adicional cuarta. *Informes consultivos del Comité técnico estatal de la Administración judicial electrónica.*

En el plazo de seis meses desde su constitución, el Comité técnico estatal de la Administración judicial electrónica entregará al Ministro de Justicia los informes que contengan el análisis jurídico y técnico necesario para el uso de los sistemas de videoconferencia en la Administración de Justicia, la universalización del acceso a los servicios electrónicos y el funcionamiento electrónico de los Archivos Judiciales de Gestión Territoriales y Central. El Comité técnico estatal de la Administración judicial electrónica, en el momento de encomendar la ejecución de dichas actividades, podrá ordenar los plazos, requisitos y condiciones de elaboración de dicho informe.

Disposición adicional quinta. *Colaboración con la procura para la práctica electrónica de actos procesales de comunicación y traslados de copias previas entre procuradores de los tribunales.*

En el plazo de un mes a contar desde la constitución del Comité técnico estatal de la Administración judicial electrónica, deberá crearse en su seno un Grupo de Trabajo, de carácter técnico y composición paritaria con el Consejo General de Procuradores de los Tribunales a los efectos de iniciar la debida colaboración que permita la ejecución de los convenios, acuerdos y proyectos necesarios para la plena y efectiva implantación de la Administración judicial electrónica, y los principios y requisitos de la misma recogidos en la Ley 18/2011, de 5 de julio, en el ámbito de la práctica de los actos procesales de comunicación y traslados de copias previas entre los Procuradores de los Tribunales y su interoperabilidad con los sistemas informáticos de gestión procesal.

En virtud de lo dispuesto en el Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones Lexnet para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos, en dicho Grupo, deberá darse oportuna participación a la Subdirección General de las Nuevas Tecnologías de la Justicia, u órgano que ejerciere sus funciones, como responsable del citado sistema informático, con independencia de la participación que el Ministerio de Justicia pudiera tener, en su condición de miembro de pleno derecho del Comité técnico estatal de la Administración judicial electrónica.

Disposición adicional sexta. *Recomendaciones de interoperabilidad y seguridad judicial en el ámbito contractual.*

El Comité técnico de la Administración judicial electrónica establecerá los mecanismos de interlocución y colaboración con los órganos superiores de contratación a fin de que la preceptiva interoperabilidad y seguridad sea contemplada en los requisitos de contratación de bienes y servicios por las Administraciones competentes en materia de Justicia. A tal efecto, podrá dictar una recomendación tipo de requisitos o condiciones a incluir en los pliegos o bases y en la evaluación que, de dicha conformidad, se realice en el procedimiento de contratación.

Disposición adicional séptima. *Colaboración con los grupos de trabajo sobre la Nueva Oficina Judicial y Nueva Oficina Fiscal.*

El Comité técnico estatal de la Administración judicial electrónica establecerá los cauces o grupos de trabajo precisos para que sus actuaciones en materia de Administración judicial electrónica estén organizadas en colaboración mutua con el Grupo de Trabajo sobre la Nueva Oficina Judicial constituido en la Conferencia Sectorial de Justicia del 7 de mayo de 2012. Dichas actuaciones y cooperación mutuas se deberán dar sin perjuicio de las funciones normativas del Comité técnico estatal de la Administración judicial electrónica previstas en el art. 51 de la Ley 18/2011, de 5 de julio, ni alteración de la composición de los órganos necesarios del Comité técnico estatal de la Administración judicial electrónica.

El Comité técnico estatal de la Administración judicial electrónica establecerá similares cauces o grupos de colaboración con los grupos de trabajo surgidos al amparo de la reunión mantenida el 27 de octubre de 2011 entre el Ministerio de Justicia y las comunidades autónomas con competencias transferidas, donde se aprobó el modelo de implantación de la nueva oficina fiscal, integrado en el Plan Estratégico de Modernización.

Disposición transitoria primera. *Continuidad de las actuaciones realizadas en el Esquema judicial de interoperabilidad y seguridad.*

Hasta el momento en que el Comité técnico estatal de la Administración judicial electrónica quede constituido, aquellos documentos, informes, recomendaciones o guías necesarias para la prosecución de las iniciativas y proyectos en materia de interoperabilidad y seguridad judicial acordados en el seno del Convenio de Colaboración entre el Ministerio de Justicia, el Consejo General del Poder Judicial y la Fiscalía General del Estado para el establecimiento del Esquema judicial de interoperabilidad y seguridad en el ámbito de la Administración de Justicia y del de aquellas comunidades autónomas con competencias en materia de Justicia adheridas al mismo, continuarán ejecutándose por la Oficina de Programa EJIS o los Grupos de Trabajo constituidos en el Consejo General del Poder Judicial de conformidad con lo dispuesto en el citado Convenio.

Disposición transitoria segunda. *Sometimiento al Comité técnico de la Administración judicial electrónica de las actuaciones realizadas en el Esquema judicial de interoperabilidad y seguridad.*

Los documentos, informes, recomendaciones o guías elaborados o publicados, en desarrollo de las previsiones de la Ley 18/2011, de 5 de julio, por los diversos Grupos de Trabajo constituidos en el seno del Convenio de Colaboración entre el Ministerio de Justicia, el Consejo General del Poder Judicial y la Fiscalía General del Estado para el

establecimiento del Esquema judicial de interoperabilidad y seguridad en el ámbito de la Administración de Justicia, serán sometidos para su aprobación a los órganos competentes del Comité, conforme a lo previsto en la Ley 18/2011, de 5 de julio, y el presente real decreto.

Disposición final primera. *Título competencial.*

El presente real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.5.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de Administración de Justicia.

Disposición final segunda. *Entrada en vigor.*

El presente real decreto entrará en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

§ 67

Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET

Ministerio de Justicia
«BOE» núm. 287, de 1 de diciembre de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-12999

Desde que fue aprobada la Ley Orgánica 16/1994, de 8 de noviembre, por la que se reformó la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y que introdujo por primera vez en nuestro ordenamiento jurídico la posibilidad de emplear medios técnicos, electrónicos e informáticos para el desarrollo de la actividad y el ejercicio de las funciones de Juzgados y Tribunales, se ha recorrido un largo camino jalonado por hitos normativos y por avances tecnológicos. Fue a mediados de los años noventa del pasado siglo cuando el uso de las nuevas tecnologías en la Administración de Justicia comenzó a extenderse de forma generalizada; desde entonces su avance no se ha detenido y han aumentado progresivamente los distintos sistemas y aplicaciones que se usan en Juzgados, Tribunales y Fiscalías para el desempeño de su actividad.

Entre los hitos normativos, se encuentra el Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones LexNET para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos. El sistema LexNET ha cumplido de manera satisfactoria las necesidades de comunicación de la Administración de Justicia con los profesionales de la justicia, principalmente con los Procuradores de los Tribunales, y preferentemente para la realización de notificaciones enviadas desde los órganos y oficinas judiciales de todos los órdenes jurisdiccionales a estos profesionales.

Posteriormente, la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, definió un marco general del uso de medios informáticos en la Administración de Justicia y dedicó el Capítulo III del Título IV al registro de escritos, las comunicaciones y las notificaciones electrónicas. Asimismo, creó el Comité técnico estatal de la Administración judicial electrónica, que actualmente ostenta las competencias en materia de interoperabilidad y compatibilidad de las distintas aplicaciones que se utilizan en la Administración de Justicia. En virtud del artículo 45 de la referida ley, este Comité ha fijado las bases de interoperabilidad y seguridad de la Administración de Justicia.

Además, a nivel europeo se ha publicado el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE para las transacciones electrónicas en el mercado interior. Este Reglamento define las condiciones para que los sistemas de

notificaciones electrónicas sean legalmente válidos en los países de la Unión Europea. Entre los objetivos de este Reglamento está reforzar la confianza en las transacciones electrónicas dentro del marco de la Unión Europea, proporcionando las herramientas jurídicas necesarias para crear un clima de seguridad entre ciudadanos, empresas y la Administración Pública, regulando el artículo 25 los efectos jurídicos de las firmas electrónicas, el 35 los del sello electrónico y los artículos 43 y 44 los efectos y requisitos de los servicios de entrega electrónica certificada.

Durante el tiempo transcurrido, en el ámbito de la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local y al amparo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, estas Administraciones han sido pioneras en el uso de las nuevas tecnologías en el ámbito de las Administraciones Públicas y se han definido en los últimos años diversos sistemas de notificaciones impulsados por varios órganos de la Administración General del Estado que, sin duda pueden ser adoptados como una posibilidad más, dentro de los límites y condiciones establecidos por las normas procesales y con sus especiales características, en el ámbito de la Administración de Justicia. Cabe destacar que en la redacción de las bases de interoperabilidad y seguridad de la Administración de Justicia se ha tomado en consideración lo establecido en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones competentes en materia de justicia y los servicios electrónicos e infraestructuras ya existentes, de conformidad con el artículo 47.3 de la Ley reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Por último, han sido aprobadas recientemente la Ley 19/2015, de 13 de julio, de medidas de reforma administrativa en el ámbito de la Administración de Justicia y del Registro Civil y la Ley 42/2015, de 5 de octubre, de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, y ambas, en sus respectivos textos, contienen disposiciones que abordan aspectos relativos a las comunicaciones telemáticas y electrónicas. En este sentido resulta de especial significado y trascendencia el contenido de la disposición adicional primera de esta última que, bajo el epígrafe «utilización de medios telemáticos», constituye singular y especifico fundamento normativo de este real decreto, regulándose en ella aspectos técnicos de especial trascendencia que afectan a ámbitos competenciales concretos y derivándose consecuencias sobre los procesos judiciales y, por tanto, sobre los derechos de los ciudadanos.

Asimismo, la fundamentación de esta norma reglamentaria se encuentra en la nueva redacción del artículo 230 de la Ley Orgánica del Poder Judicial, que establece la obligación de los Juzgados y Tribunales y también de las Fiscalías de utilizar cualesquiera medios técnicos electrónicos, informáticos y telemáticos puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, siempre con las limitaciones legales que resulten de aplicación.

Este real decreto también encuentra su base legal en los artículos 4 y 6 de la Ley 18/2011, de 5 de julio, que establecen respectivamente el derecho de elección del ciudadano del canal a través del cual relacionarse con la Administración de Justicia y, en su caso, a elegir las aplicaciones y sistemas para hacerlo electrónicamente, y el derecho y deber de los profesionales de la justicia a relacionarse con ésta mediante canales electrónicos. No obstante, esta Ley ha sido modificada por la Ley de reforma de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, disponiendo la posibilidad de que legal o reglamentariamente se establezca la obligatoriedad de comunicarse con la Administración de Justicia solo por medios electrónicos cuando se trate de personas jurídicas o colectivos de personas físicas que por razón de su capacidad económica o técnica, dedicación profesional u otros motivos acreditados tengan garantizado el acceso y disponibilidad de los medios tecnológicos precisos.

Este real decreto se dicta haciendo uso de la habilitación contenida en el apartado 2 de la disposición adicional primera de la Ley Orgánica del Poder Judicial, así como de la que establece, respecto al ámbito competencial del Ministerio de Justicia, la disposición final segunda de la Ley 18/2011, de 5 de julio.

Finalmente, en el proceso de elaboración de este real decreto han emitido informe, entre otros, el Consejo General del Poder Judicial, el Consejo Fiscal, el Comité Técnico Estatal de la Administración Judicial electrónica y la Agencia Española de Protección de Datos.

En su virtud, a propuesta del Ministro de Justicia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 27 de noviembre de 2015,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente real decreto tiene por objeto desarrollar la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, en lo relativo a las comunicaciones y notificaciones electrónicas, así como a la presentación electrónica de escritos, documentos u otros medios o instrumentos y al traslado de copias, en el ámbito de la competencia del Ministerio de Justicia y sin perjuicio de las competencias asumidas por las Comunidades Autónomas.

2. Sus disposiciones serán de aplicación:

a) A todos los integrantes de los órganos y oficinas judiciales y fiscales.

b) A todos los profesionales que actúan en el ámbito de la Administración de Justicia.

c) A las relaciones entre los órganos y oficinas judiciales y fiscales y los órganos técnicos que les auxilian y el resto de Administraciones y organismos públicos y las Fuerzas y Cuerpos de Seguridad.

d) A las personas que por ley o reglamento estén obligadas a intervenir a través de medios electrónicos con la Administración de Justicia.

e) A los ciudadanos que ejerzan el derecho a relacionarse con la Administración de Justicia a través de medios electrónicos.

Artículo 2. *Definiciones.*

A los efectos de este real decreto se entenderá por:

a) Integrantes de los órganos y oficinas judiciales y fiscales: los miembros de la Carrera Judicial y Fiscal y los funcionarios del Cuerpo Superior Jurídico de Letrados de la Administración de Justicia y de los Cuerpos de Médicos Forenses, de Facultativos del Instituto Nacional de Toxicología y Ciencias Forenses, de Gestión Procesal y Administrativa, de Técnicos Especialistas del Instituto Nacional de Toxicología y Ciencias Forenses, de Tramitación Procesal y Administrativa, de Auxilio Judicial y de Ayudantes de Laboratorio del Instituto Nacional de Toxicología y Ciencias Forenses, así como los equipos técnicos que presten soporte a la actividad judicial.

b) Profesionales de la justicia: profesionales que actúan en el ámbito de la Administración de Justicia. En concreto, Abogados, Procuradores, Graduados Sociales, Cuerpo de Abogados del Estado, Letrados de las Cortes Generales y de las Asambleas Legislativas y Letrados del Servicio Jurídico de la Administración de la Seguridad Social, de las demás Administraciones públicas, de las Comunidades Autónomas o de los Entes Locales, así como los Colegios de Procuradores.

También tendrán la consideración de profesionales de la justicia a estos efectos los administradores concursales.

c) Presentaciones electrónicas: la aportación, presentación o remisión a los órganos y oficinas judiciales y fiscales de toda clase de escritos, solicitudes, documentos, dictámenes, informes u otros medios, instrumentos o expedientes por parte de los ciudadanos, profesionales de la justicia, Administraciones y organismos públicos y Fuerzas y Cuerpos de Seguridad a través un canal electrónico. También las presentaciones realizadas por los órganos y oficinas judiciales y fiscales en los supuestos legalmente previstos.

d) Comunicaciones y notificaciones electrónicas: la realización mediante un canal electrónico de los actos de comunicación procesal emanados de los órganos y oficinas

judiciales, tales como notificaciones, citaciones, emplazamientos, requerimientos, mandamientos, oficios y exhortos. Asimismo, los actos de comunicación emanados de los órganos y oficinas fiscales, de los Institutos de Medicina Legal y Ciencias Forenses, del Instituto Nacional de Toxicología y Ciencias Forenses y de los equipos técnicos que presten soporte a la actividad judicial, en los supuestos legalmente previstos.

e) Información en soporte digital o electrónico: toda información digitalizada y almacenada en un medio electrónico de forma que permita su tramitación y transmisión de forma electrónica de acuerdo a la Ley 18/2011, de 5 de julio.

f) Transmisión electrónica de información: transmisión a distancia de datos incorporados en documentos o archivos de otro tipo que se realiza mediante el uso de un canal electrónico.

g) Canal electrónico: todo canal de transmisión de datos por medios electrónicos, ópticos o de radiofrecuencia.

Artículo 3. *Presentaciones, comunicaciones y notificaciones electrónicas.*

1. Las presentaciones y las comunicaciones y notificaciones realizadas por canales electrónicos deberán ajustarse a las normas procesales.

2. Los sistemas electrónicos de información y comunicación deberán dejar constancia de la transmisión y recepción de las presentaciones y de las comunicaciones y notificaciones, de la fecha y hora en que se produzca su salida y de las de la puesta a disposición del interesado, de su contenido íntegro y del acceso al mismo, así como de la identificación del remitente y del destinatario de las mismas. Los sistemas de identificación y autentificación se ajustaran a lo previsto en la Ley 18/2011, de 5 de julio, en la Ley 59/2003, de 19 de diciembre, de firma electrónica, en el Reglamento UE n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y en el presente real decreto.

3. Todos los sistemas electrónicos de información y comunicación deberán regirse por las Bases del Esquema judicial de interoperabilidad y seguridad. Para ello, todas las aplicaciones y sistemas que se utilicen para comunicarse con la Administración de Justicia deberán hacer uso de las guías de interoperabilidad y seguridad de las tecnologías de la información y las comunicaciones elaboradas por el Comité técnico estatal de la Administración judicial electrónica, en especial de las guías de documento y expediente judicial electrónico, así como de la de política de firma.

Artículo 4. *Derecho de los ciudadanos a elegir y obligatoriedad de las presentaciones y de las comunicaciones y notificaciones electrónicas.*

Los ciudadanos que no estén asistidos o representados por profesionales de la justicia podrán elegir, en todo momento, que la manera de comunicarse con la Administración de Justicia y la forma de recibir las comunicaciones y notificaciones de la misma sea o no por canales electrónicos.

No obstante, estarán obligados a comunicarse con la Administración de Justicia, en todo caso, a través de canales electrónicos, los siguientes sujetos:

a) Las personas jurídicas.

b) Las entidades sin personalidad jurídica.

c) Quienes ejerzan una actividad profesional para la que se requiera colegiación obligatoria para los trámites y actuaciones que realicen con la Administración de Justicia en ejercicio de dicha actividad profesional.

d) Los Notarios y Registradores.

e) Quienes representen a un interesado que esté obligado a relacionarse electrónicamente con la Administración de Justicia.

f) Los funcionarios de las Administraciones Públicas para los trámites y actuaciones que realicen por razón de su cargo.

g) Y los que legal o reglamentariamente se establezcan.

Artículo 5. *Obligatoriedad para los profesionales de la justicia y los órganos y oficinas judiciales y fiscales.*

1. Todos los Abogados, Procuradores, Graduados Sociales, Abogados del Estado, Letrados de las Cortes Generales, de las Asambleas Legislativas y del Servicio Jurídico de la Administración de la Seguridad Social, de las demás Administraciones Públicas, de las Comunidades Autónomas o de los Entes Locales, así como los Colegios de Procuradores y administradores concursales tienen la obligación de utilizar los sistemas electrónicos existentes en la Administración de Justicia para la presentación de escritos y documentos y para la recepción de actos de comunicación.

2. Asimismo, los sistemas electrónicos de información y comunicación, al igual que el resto de sistemas informáticos puestos al servicio de la Administración de Justicia, deben ser usados obligatoriamente para el desempeño de su actividad por todos los integrantes de los órganos y oficinas judiciales y fiscales.

Artículo 6. *Formas de identificación y autenticación.*

1. Para el empleo de los sistemas electrónicos de información y comunicación que así lo requieran serán válidos los sistemas de identificación electrónica y de firma electrónica que sean conformes a lo establecido por la Ley 59/2003, de 19 de diciembre, de firma electrónica, y el Reglamento UE n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE, y resulten adecuados para garantizar la identificación de los intervinientes y, en su caso, la autenticidad e integridad de los documentos electrónicos.

2. La Administración de Justicia podrá utilizar para su identificación electrónica y para la autenticación de los documentos electrónicos que produzca sistemas de firma electrónica para la actuación judicial automatizada, sistemas basados en certificados electrónicos del personal al servicio de la Administración de Justicia y otros sistemas de firma que permitan atribuir la firma al firmante y comprobar la autenticidad de documentos en base a Códigos Seguros de Verificación.

Asimismo, podrán utilizarse, en su caso, sistemas de identificación, autenticación y firma electrónica mediante el uso de claves concertadas reutilizando las plataformas del sector público administrativo estatal.

3. Las personas jurídicas y entidades sin personalidad jurídica podrán utilizar sistemas basados en certificados electrónicos de persona jurídica o de entidad sin personalidad jurídica, así como sellos electrónicos avanzados basados en certificados cualificados.

4. El uso de la firma electrónica no excluye la obligación de incluir en los documentos o en las comunicaciones electrónicas los datos de identificación del firmante y, en su caso, de la persona o entidad a la que represente y los que sean necesarios de acuerdo con la legislación aplicable.

Artículo 7. *Seguridad en las presentaciones, comunicaciones y notificaciones electrónicas.*

1. Para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en las presentaciones y en las comunicaciones y notificaciones electrónicas en la Administración de Justicia se aplicará el Esquema judicial de interoperabilidad y seguridad.

2. Los sistemas electrónicos de información y comunicación deberán cumplir los requisitos mínimos de seguridad fijados en las Bases del Esquema judicial de interoperabilidad y seguridad. Estos requisitos, de conformidad con lo previsto en el artículo 54 de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, serán desarrollados mediante una guía técnica de seguridad, en línea con lo establecido en las Instrucciones Técnicas de Seguridad de la Administración General del Estado.

3. Lo dispuesto en este real decreto se aplicará observando y garantizando la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

CAPITULO II

Presentaciones, traslado de copias, comunicaciones y notificaciones electrónicas

Artículo 8. *Canales electrónicos.*

1. La presentación de escritos y documentos, el traslado de copias y la realización de comunicaciones y notificaciones por medios electrónicos se efectuaran a través del sistema LexNET o mediante la sede judicial electrónica correspondiente.

2. Los ciudadanos que no estando asistidos o representados por profesionales de la justicia opten por comunicarse con la Administración de Justicia por medios electrónicos o estén obligados a ello podrán usar el Servicio Compartido de Gestión de Notificaciones Electrónicas y la Carpeta Ciudadana provistos por el Ministerio de Hacienda y Administraciones Públicas siempre que los medios tecnológicos lo permitan.

3. Los Colegios de Procuradores habilitarán los medios necesarios para garantizar la presentación de escritos y documentos, el traslado de copias y la recepción de los actos de comunicación por medios electrónicos, por todos sus profesionales en cualquier parte del territorio nacional, independientemente del Colegio de Procuradores de adscripción al que pertenezcan.

Artículo 9. *Presentación de escritos y documentos por canales electrónicos.*

1. Los órganos y las oficinas judiciales y fiscales, así como los profesionales de la justicia, remitirán sus escritos y documentos a través del sistema LexNET.

Las Administraciones y organismos públicos y las Fuerzas y Cuerpos de Seguridad también podrán usar los servicios de la sede judicial electrónica que se habiliten expresamente para ellas.

2. Cuando, de conformidad con lo dispuesto por las normas procesales, no sea preceptiva la asistencia letrada ni la representación por Procurador o, en su caso, Graduado Social, los ciudadanos que opten por relacionarse con la Administración de Justicia por medios electrónicos y las personas que vengan obligadas a ello conforme a las leyes o reglamentos utilizarán para la presentación de escritos y documentos la sede judicial electrónica. También podrán utilizar el Servicio Compartido de Gestión de Notificaciones Electrónicas y la Carpeta Ciudadana provistos por el Ministerio de Hacienda y Administraciones Públicas siempre que los medios tecnológicos lo permitan.

3. La presentación de toda clase de escritos, documentos, dictámenes, informes u otros medios o instrumentos deberá ir acompañada de un formulario normalizado con el detalle o índice comprensivo del número, orden y descripción somera del contenido de cada uno de los documentos, así como, en su caso, del órgano u oficina judicial o fiscal al que se dirige y el tipo y número de expediente y año al que se refiere el escrito. Este formulario normalizado se ajustará a las disposiciones del Reglamento 2/2010, sobre criterios generales de homogeneización de las actuaciones de los servicios comunes procesales, aprobado por Acuerdo, de 25 de febrero de 2010, del Pleno del Consejo General del Poder Judicial.

Artículo 10. *Traslado de copias electrónicas.*

1. Cuando la presentación de escritos y documentos se realice por Procuradores y además deba efectuarse el traslado de copias en los términos previstos en el artículo 276 y siguientes de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, podrá llevarse a cabo a través de la plataforma del Consejo General de Procuradores de España aprobada técnicamente por el Ministerio de Justicia y conectada a LexNET.

En caso de que el traslado de copias entre Procuradores se realice a través de la plataforma del Consejo General de Procuradores de España, la presentación electrónica que se dirija al órgano u oficina judicial o fiscal deberá contener un justificante firmado electrónicamente que acredite de forma inequívoca que el traslado de copias se ha realizado observando las disposiciones procesales.

2. La obligación de realizar el traslado de copias de escritos y documentos cuando intervengan Procuradores será igualmente exigible, en los términos previstos en los artículos

276 y siguientes de la Ley de Enjuiciamiento Civil, en los órdenes jurisdiccionales penal, contencioso-administrativo y social.

Artículo 11. *Comunicaciones y notificaciones por canales electrónicos.*

1. Los órganos y oficinas judiciales y fiscales realizarán los actos de comunicación con las partes procesales y, en su caso, con los terceros intervinientes, mediante los siguientes canales electrónicos:

a) El sistema LexNET, si se trata, en su caso, de otros órganos y oficinas judiciales y fiscales, cuando las partes intervinientes en el proceso estén representadas por profesionales de la justicia y así lo permitan las normas procesales y cuando los destinatarios de los actos de comunicación sean las Administraciones y organismos públicos y las Fuerzas y Cuerpos de Seguridad.

b) La sede judicial electrónica.

c) El Servicio Compartido de Gestión de Notificaciones Electrónicas y la Carpeta Ciudadana provistos por el Ministerio de Hacienda y Administraciones Públicas siempre que los medios tecnológicos lo permitan.

d) Otros sistemas electrónicos de información y comunicación que puedan establecerse.

2. Será de aplicación a los actos de comunicación realizados a través de la sede judicial electrónica lo dispuesto en el artículo 162.2 de la Ley de Enjuiciamiento Civil.

3. Todos estos medios deberán cumplir los requisitos de autenticidad, integridad, temporalidad y resguardo acreditativo en los procesos de envío y recepción.

Artículo 12. *Disponibilidad de los sistemas electrónicos.*

1. Los medios electrónicos relacionados en los artículos anteriores estarán en funcionamiento durante las veinticuatro horas del día, todos los días del año, sin perjuicio de lo previsto en el apartado siguiente de este artículo. En ningún caso la presentación electrónica de escritos y documentos o la recepción de actos de comunicación por medios electrónicos implicará la alteración de lo establecido en las leyes sobre el tiempo hábil para las actuaciones procesales, plazos y su cómputo, ni tampoco supondrá ningún trato discriminatorio en la tramitación y resolución de los procesos y actuaciones ante los órganos y oficinas judiciales y fiscales.

2. Cuando la presentación de escritos y documentos dentro de plazo por los medios electrónicos no sea posible por interrupción no planificada del servicio de comunicaciones electrónicas, siempre que sea factible se dispondrán las medidas para que el usuario resulte informado de esta circunstancia, así como de los efectos de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. El remitente podrá proceder, en este caso, a su presentación en el órgano u oficina judicial o fiscal el primer día hábil siguiente acompañando el justificante de dicha interrupción.

En los casos de interrupción planificada por la ineludible realización de trabajos de mantenimiento u otras razones técnicas lo requieran, podrán planificarse paradas de los sistemas informáticos que afecten o imposibiliten de forma temporal el servicio de comunicaciones electrónicas. Estas paradas serán avisadas por el propio sistema informático con una antelación mínima de veinte días, indicando el tiempo estimado de indisponibilidad del servicio. Este plazo podrá ser reducido en caso de aplicación de medidas de seguridad y otras necesidades de corrección urgente.

CAPITULO III

Sistema LexNET

Artículo 13. *Definición y características.*

1. El sistema LexNET es un medio de transmisión seguro de información que mediante el uso de técnicas criptográficas garantiza la presentación de escritos y documentos y la recepción de actos de comunicación, sus fechas de emisión, puesta a disposición y recepción o acceso al contenido de los mismos.

Asimismo, el sistema LexNET garantiza el contenido íntegro de las comunicaciones y la identificación del remitente y destinatario de las mismas mediante técnicas de autenticación adecuadas, de conformidad con lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y en el Reglamento UE Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

2. El sistema LexNET tendrá la consideración de sistema de entrega electrónica certificada conforme al artículo 43 del Reglamento UE nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

3. Cuando el envío proceda de una Administración u organismo público y de las Fuerzas y Cuerpos de Seguridad podrá utilizarse el sistema de acceso mediante usuario y contraseña, siempre que la comunicación se realice a través de los Sistemas de Aplicaciones y Redes para las Administraciones.

Artículo 14. *Funcionalidades del sistema LexNET.*

El sistema LexNET prestará las siguientes funcionalidades:

a) La presentación y transporte de escritos procesales y documentos que con los mismos se acompañen, así como su distribución y remisión al órgano u oficina judicial o fiscal encargada de su tramitación.

b) La gestión del traslado de copias, de modo que quede acreditado en las copias la fecha y hora en que se ha realizado efectivamente el traslado a los restantes Procuradores personados y la identidad de éstos, de conformidad con lo previsto en las leyes procesales.

c) La realización de actos de comunicación procesal conforme a los requisitos establecidos en las leyes procesales.

d) La expedición de resguardos electrónicos, integrables en las aplicaciones de gestión procesal, acreditativos de la correcta realización de la presentación de escritos y documentos anexos, de los traslados de copias y de la remisión y recepción de los actos de comunicación procesal y, en todo caso, de la fecha y hora de la efectiva realización.

e) La constancia de un asiento por cada una de las transacciones electrónicas a que se refieren los números anteriores, realizadas a través del sistema, identificando cada transacción los siguientes datos: identidad del remitente y del destinatario de cada mensaje, fecha y hora de su efectiva realización proporcionada por el sistema y, en su caso, proceso judicial al que se refiere, indicando tipo de procedimiento, número y año.

Artículo 15. *Administración del sistema.*

1. El Ministerio de Justicia, encargado de administrar y mantener el entorno operativo y disponibilidad del sistema, podrá suscribir convenios de cooperación tecnológica con las Comunidades Autónomas que hayan recibido los traspasos de funciones y servicios en relación con los medios materiales de la Administración de Justicia, para la implantación del sistema electrónico denominado LexNET en sus ámbitos territoriales correspondientes. Dichos convenios se ajustarán a las características del sistema y respetarán las garantías establecidas en este real decreto.

El Ministerio de Justicia pondrá a disposición de todas las Comunidades Autónomas a las que se refiere el párrafo anterior el sistema de telecomunicaciones LexNET.

El Ministerio de Justicia tendrá la responsabilidad de garantizar el correcto funcionamiento, la custodia y la seguridad del sistema, sin perjuicio de las atribuciones correspondientes a las Comunidades Autónomas que hayan recibido los traspasos de funciones y servicios en relación con los medios materiales de la Administración de Justicia en los términos de los convenios de cooperación tecnológica suscritos con estas.

2. El Consejo General de la Abogacía Española y el Consejo General de Procuradores de España podrán conectar sus plataformas con el sistema LexNET siempre que esta conexión sea aprobada técnicamente por el Ministerio de Justicia y permita la interoperabilidad completa con dicho sistema. Estas interconexiones estarán dirigidas a facilitar a los profesionales de la justicia a ellos adscritos el cumplimiento de las obligaciones

establecidas en el artículo 162 de la Ley de Enjuiciamiento Civil y de los deberes contemplados en la Ley 18/2011, de 5 de julio.

Los Consejos Generales que se interconecten con LexNET deberán mantener sus plataformas y aplicaciones interoperables con el sistema LexNET.

La actualización e interoperabilidad de los sistemas de los Consejos Generales será competencia exclusiva de los mismos.

Artículo 16. *Disponibilidad del sistema LexNET.*

1. Cuando por cualquier causa, el sistema LexNET o las plataformas del Consejo General de la Abogacía Española y del Consejo General de Procuradores de España aprobadas técnicamente por el Ministerio de Justicia y conectadas a LexNET no pudieran prestar el servicio en las condiciones establecidas, se informará a los usuarios a los efectos de la eventual presentación de escritos y documentos y traslado de copias, así como de la realización de los actos de comunicación en forma no electrónica y se expedirá, previa solicitud, justificante de la interrupción del servicio o certificado del Consejo General Profesional correspondiente expresivo de tal imposibilidad, el tiempo que permaneció inactivo y las causas. El justificante y los certificados que expidan los Consejos Generales Profesionales surtirán los efectos previstos en el párrafo segundo del artículo 162.2 de la Ley de Enjuiciamiento Civil, a fin de que el destinatario de las comunicaciones pueda justificar la falta de acceso al sistema por causas técnicas durante ese periodo.

2. Antes de acceder el destinatario al detalle del contenido del envío, el sistema LexNET mostrará, al menos, la información esencial relativa al remitente del envío, asunto, clase y número de procedimiento en su caso, así como fecha de envío. Para que aquel pueda acceder al contenido de la comunicación previamente deberá proceder a su aceptación.

3. Una vez depositados en los buzones virtuales de los usuarios los escritos, las comunicaciones y notificaciones, así como cualquier otro documento procesal transmitido por medios electrónicos, se encontrarán accesibles por un período de sesenta días. Transcurrido este plazo se procederá a la eliminación del buzón de estos documentos, salvo los resguardos electrónicos acreditativos de la transmisión.

4. Para conseguir una adecuada gestión y tratamiento por los destinatarios de las comunicaciones y notificaciones electrónicas, cuando se produzca una acumulación masiva de las mismas a enviar después de un periodo inhábil o por concurrir circunstancias excepcionales, el propio sistema impedirá que se supere en más de un cincuenta por ciento al día el volumen de salida ordinario de actos de comunicación y, si técnicamente no fuera posible, los responsables del envío adoptaran las medidas necesarias a tal fin, repartiendo de forma gradual el exceso acumulado en remisiones consecutivas durante los cinco días posteriores al periodo de inhabilidad o al cese de la circunstancia excepcional.

5. Los mecanismos técnicos que aseguren la confidencialidad de la información procesal transmitida garantizarán que el administrador del sistema no tenga acceso a su contenido.

6. No obstante, la custodia de la información acreditativa de las transacciones realizadas a través del sistema LexNET corresponde al administrador del sistema, en las condiciones establecidas en el Fichero 1 «Custodia de la información acreditativa de las transacciones realizadas», del Anexo I.

Artículo 17. *Operativa funcional del sistema en las presentaciones, traslado, comunicaciones y notificaciones electrónicas.*

1. La presentación de escritos y documentos procesales iniciadores y de trámite, el traslado de copias cuando intervenga Procurador y la realización de actos de comunicación a través del sistema LexNET requerirá por parte de los usuarios del sistema la previa cumplimentación de todos los campos de datos obligatorios que aparecen relacionados en el Anexo III, y que deberán ser coincidentes con los del formulario previsto en los artículos 36.4 y 38.1 de la Ley 18/2011, de 5 de julio.

2. El usuario podrá incorporar, además del documento electrónico principal, en el que se contenga el propio acto procesal objeto de transmisión, otros anexos, uno por cada uno de los documentos electrónicos que se deban acompañar. El usuario podrá visualizar los documentos electrónicos incorporados como anexos, a efectos de comprobación, antes de proceder a su envío.

En su caso, se acompañarán también aquellos elementos que no sean susceptibles de conversión en formato electrónico y las copias en soporte papel para realizar el acto de comunicación o traslado de copias a las partes no personadas.

Los usuarios del sistema presentarán sus escritos utilizando firma electrónica cualificada. Los documentos electrónicos anexos también serán firmados electrónicamente mediante certificado electrónico reconocido o cualificado.

Cuando, por las singulares características de un documento, el sistema no permita su incorporación como anexo para su envío en forma electrónica, el usuario hará llegar dicha documentación al destinatario por otros medios, en la forma establecida en las normas procesales y en el artículo siguiente, y deberá hacer referencia a los datos identificativos del envío electrónico al que no pudo ser adjuntada.

3. Para la acreditación de la presentación de los escritos y documentos y la realización de los actos de comunicación, el sistema devolverá al usuario un resguardo electrónico acreditativo de la remisión y puesta a disposición de la documentación, de su recepción por el destinatario, de la descripción de cada uno de los documentos transmitidos, de la identificación del remitente o profesional que le sustituye y del destinatario, del tipo de procedimiento judicial, número y año, así como de la fecha y hora de su efectiva realización o de cualquier otra información que se estime relevante en orden a constatar la certeza de la presentación o realización de dicho acto de comunicación.

4. Para el traslado de copias entre Procuradores, los Colegios de Procuradores utilizarán medios electrónicos que cumplan las previsiones del artículo 276 de la Ley de Enjuiciamiento Civil, permitan el envío y la recepción de copias de escritos y documentos de forma simultánea a la presentación de los escritos de trámite, de tal modo que esté garantizada la autenticidad de la comunicación y de su contenido, y quede constancia fehaciente de la remisión y recepción íntegras y del momento en que se hicieron, con el resguardo acreditativo de su recepción que proceda.

La plataforma del Consejo General de Procuradores de España aprobada técnicamente por el Ministerio de Justicia permitirá la realización del traslado de copias de escritos y documentos por cualquier Procurador en cualquier parte del territorio nacional y con independencia del Colegio de Procuradores de adscripción.

5. El sistema confirmará al usuario la recepción del mensaje por el destinatario. La falta de confirmación no implicará que no se haya producido la recepción. En aquellos casos en que se detecten anomalías en la transmisión electrónica o no haya sido posible completar el envío, el propio sistema lo pondrá en conocimiento del usuario, mediante los correspondientes mensajes de error, para que proceda a la subsanación o realice el envío en otro momento o utilizando otros medios.

El mensaje de error o deficiencia de la transmisión podrá ser imprimido o archivado por el usuario y, si el sistema lo permite, integrado en los sistemas de gestión procesal a efectos de acreditación del intento fallido.

En los casos en que se haya producido un error en la recepción e incorporación a los sistemas de gestión procesal y se haya subsanado el mismo en tiempo y forma, dentro de los cauces previstos por el sistema, este expedirá un resguardo acreditativo de la subsanación correspondiente, respetando la fecha y hora del envío inicialmente realizado.

Artículo 18. *Limitaciones por el volumen o formato de los archivos adjuntos.*

Cuando por el exceso del volumen de los archivos adjuntos, por el formato de éstos o por la insuficiencia de capacidad del sistema LexNET, el sistema no permita su inclusión, impidiendo el envío en forma conjunta con el escrito principal, se remitirá únicamente el escrito a través del sistema electrónico y el resto de documentación, junto con el formulario normalizado previsto en el último párrafo del artículo 9 o, en su defecto, el índice con el número, clase y descripción de los documentos y el acuse de recibo de dicho envío emitido por el sistema, se presentará en soporte digital o en cualquier otro tipo de medio electrónico que sea accesible para los órganos y oficinas judiciales y fiscales, ese día o el día hábil inmediatamente posterior a la fecha de realización del envío principal, en el órgano u oficina judicial o fiscal correspondiente. En estos casos, los archivos deberán ser analizados con software antivirus antes de proceder a su volcado en los sistemas de gestión procesal por el personal de este.

Artículo 19. *Sustituciones y autorizaciones de los profesionales de la justicia.*

1. El sistema LexNET permitirá en la presentación de los escritos y documentos, traslado de copias y recepción de los actos de comunicación, la sustitución entre los profesionales de la justicia que sean de la misma profesión o cuerpo, cuando así lo prevean sus normas estatutarias.

2. El alta en el sistema LexNET para los profesionales de la justicia implicará la titularidad sobre un buzón virtual. El titular de cada buzón podrá vincular al mismo a otros usuarios como autorizados para que en su nombre puedan realizar con plenitud de efectos jurídicos los envíos de documentación o recepción de actos de comunicación desde ese buzón. Los usuarios autorizados deberán acceder, en todo caso, mediante su propio certificado electrónico. El sistema garantizará la auditoría acerca de las personas que tuvieron acceso al buzón y en qué momento, las acciones realizadas por el usuario titular o autorizado y el resultado de las mismas.

No obstante lo anterior, en las presentaciones de escritos y documentos, estos deberán haber sido firmados previamente por el titular del buzón con su certificado electrónico aunque la remisión se ejecute materialmente por un usuario autorizado por aquel.

CAPITULO IV

Sede judicial electrónica

Artículo 20. *Presentación de escritos y documentos a través de la sede judicial electrónica.*

Los ciudadanos que, no siendo preceptiva su representación o asistencia por profesionales de la justicia, opten por relacionarse con la Administración de Justicia por medios electrónicos o vengan obligados a ello por ley o reglamento presentarán los escritos, demandas, solicitudes y documentos en los formatos y con las características que se describen en el Anexo IV, a los órganos y oficinas judiciales y fiscales a través de la sede judicial electrónica, salvo que utilicen el Servicio Compartido de Gestión de Notificaciones Electrónicas y la Carpeta Ciudadana provistos por el Ministerio de Hacienda y Administraciones Públicas si los medios tecnológicos lo permiten.

Artículo 21. *Comunicaciones y notificaciones por comparecencia electrónica.*

1. A través de la sede judicial electrónica correspondiente se prestará el servicio de comunicación y notificación por comparecencia electrónica al ciudadano. En este caso, el ciudadano debidamente identificado podrá acceder al contenido de la resolución procesal objeto de comunicación y notificación.

2. El servicio de notificación por comparecencia electrónica deberá cumplir los siguientes requisitos:

a) Inmediatamente antes de acceder al contenido del acto de comunicación, el interesado deberá visualizar un aviso del carácter de notificación, citación, emplazamiento o requerimiento que contendrá dicho acceso.

b) El sistema electrónico de información y comunicación correspondiente dejará constancia de dicho acceso con indicación de fecha y hora.

3. Con la finalidad de facilitar la realización del acto de comunicación, el ciudadano podrá facilitar un número de teléfono móvil o dirección de correo electrónico habitual para recibir en ellos un aviso de puesta a su disposición de un acto de comunicación por comparecencia electrónica al que podrá acceder y consultar desde Internet.

Artículo 22. *Comunicaciones y notificaciones mediante dirección electrónica habilitada.*

1. También a través de la sede judicial electrónica podrán realizarse los actos de comunicación emanados de los órganos y oficinas judiciales y fiscales mediante la dirección electrónica habilitada. Para ello los ciudadanos podrán solicitar la apertura de esta dirección electrónica que permitirá:

a) Acreditar el momento en que se pone a disposición de la parte procesal el contenido de la resolución a comunicar.

b) Dejar constancia de la fecha y hora de acceso a su contenido.

c) Garantizar la identidad de usuario y su uso exclusivo por el mismo.

2. La dirección electrónica habilitada tendrá vigencia indefinida, excepto en los supuestos que sea solicitada su revocación por su titular, por fallecimiento de la persona física, extinción de la personalidad jurídica o disolución de la entidad sin personalidad, por resolución judicial que así lo ordene, o por el transcurso de cinco años sin ser utilizada para realizar acto de comunicación alguno.

Artículo 23. *Comunicación y notificación mediante correo electrónico.*

Los órganos y oficinas judiciales y fiscales podrán realizar actos de comunicación en las direcciones de correo electrónico que los ciudadanos elijan siempre que en el momento del acceso al contenido de la comunicación se genere automáticamente y de forma independiente a la voluntad del ciudadano un acuse de recibo acreditativo del día y hora de la remisión del acto de comunicación y de la recepción integra de su contenido y de los documentos adjuntos.

El ciudadano deberá ser advertido expresamente que solo podrá optar por el correo electrónico como medio preferente de comunicación con la Administración de Justicia si este genera un acuse de recibo del acceso al contenido del mensaje.

Artículo 24. *Comunicación y notificación edictal.*

Se publicarán en el tablón edictal de la sede o subsede judicial electrónica aquellas resoluciones y actos de comunicación que requieran por disposición legal su publicación en el tablón de anuncios del órgano u oficina judicial y fiscal.

Cualquier tratamiento ulterior de la información publicada en el tablón edictal estará sometida a la Ley 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal y a sus disposiciones de desarrollo.

Los sistemas de búsqueda que se implanten en el tablón edictal contarán con los mecanismos necesarios para evitar la indexación de la información contenida en el tablón y recuperación automática de los anuncios publicados por medio de motores de búsqueda desde Internet.

Artículo 25. *Mensajes de texto.*

Las partes procesales y terceros intervinientes en los procesos podrán proporcionar números de dispositivos electrónicos, teléfonos móviles, o direcciones de correo electrónico a través de los que puedan ponerse en contacto los órganos y oficinas judiciales y fiscales con el fin de que les sean remitidos mensajes de texto o avisos de apoyo a los actos de comunicación y que identifiquen página web o enlace donde se encuentre a disposición del destinatario el acto de comunicación y la documentación correspondiente, pero nunca con efectos procesales.

Disposición adicional primera. *Sistema informático para la presentación de escritos, traslado de copias y realización de actos de comunicación en la Jurisdicción Militar.*

La implantación del sistema LexNET en la Jurisdicción Militar y en la Fiscalía Jurídica Militar se realizará de forma conjunta por los Ministerios de Justicia y de Defensa mediante los instrumentos de colaboración que resulten más eficaces para tal fin.

Disposición adicional segunda. *Modelo de formulario normalizado.*

El Ministerio de Justicia aprobará, mediante resolución del titular de la Secretaría General de la Administración de Justicia, el modelo de formulario normalizado previsto en el apartado 3 del artículo 9.

Disposición adicional tercera. *Garantías de accesibilidad a los servicios electrónicos.*

El Ministerio de Justicia procurará que todos los ciudadanos, con especial atención a las personas mayores o con discapacidad, que se relacionan con la Administración de Justicia puedan acceder a los sistemas electrónicos de información y comunicación en igualdad de condiciones, con independencia de sus circunstancias personales, medios o conocimientos.

Disposición transitoria primera. *Vigencia de los convenios de colaboración suscritos para la utilización del sistema LexNET.*

Los convenios de colaboración para la utilización del sistema LexNET suscritos con anterioridad a la entrada en vigor de este real decreto por el Ministerio de Justicia con otras Administraciones públicas conservarán su vigencia hasta su vencimiento o denuncia por cualquiera de las partes, siendo igualmente susceptibles de ser prorrogados en los términos y condiciones estipulados en cada uno de ellos.

Disposición transitoria segunda. *Uso del correo electrónico como servicio de entrega electrónica certificada.*

Hasta que el ciudadano que opte por el uso del correo electrónico como medio preferente de comunicación con la Administración de Justicia no disponga de un sistema que genere un acuse de recibo del acceso al contenido del mensaje, los órganos y oficinas judiciales y fiscales prestarán el servicio de comunicación y notificación al ciudadano que elija este medio, en todos los órdenes jurisdiccionales, a través de sede judicial electrónica.

En estos supuestos, la dirección de correo electrónico facilitada servirá a los órganos y oficinas judiciales y fiscales como medio de apoyo para remitir al destinatario aviso de la realización del acto de comunicación y que identifique página web o enlace donde se encuentre a disposición del destinatario el acto de comunicación y la documentación correspondiente, pero nunca con efectos procesales.

Disposición transitoria tercera. *Incorporación de los administradores concursales al sistema LexNET.*

Los administradores concursales, hasta el día siguiente a la publicación del desarrollo reglamentario sobre el régimen de la administración concursal previsto en la disposición transitoria segunda de la Ley 17/2014, de 30 de septiembre, por la que se adoptan medidas urgentes en materia de refinanciación y reestructuración de deuda empresarial, seguirán comunicándose con la Administración de Justicia por medio de soporte papel. A partir de esa fecha estarán obligados a la presentación de escritos y a la recepción de las comunicaciones y notificaciones por el sistema LexNET.

Disposición derogatoria única. *Derogación normativa.*

Queda derogado el Real Decreto 84/2007, de 26 de enero, sobre implantación en la Administración de Justicia del sistema informático de telecomunicaciones LexNET para la presentación de escritos y documentos, el traslado de copias y la realización de actos de comunicación procesal por medios telemáticos.

Disposición final primera. *Título competencial.*

El presente real decreto se dicta al amparo de lo dispuesto en el artículo 149.1.5.ª de la Constitución Española, que atribuye al Estado la competencia exclusiva en materia de Administración de Justicia.

Disposición final segunda. *Facultad de desarrollo.*

1. Se faculta al Ministerio de Justicia para dictar las disposiciones necesarias para la aplicación y desarrollo de este real decreto.

2. Asimismo, se habilita al Ministro de Justicia para modificar los ficheros automatizados de datos de carácter personal contenidos en el Anexo I, variar la relación de usuarios que se reflejan en el Anexo II, modificar y aprobar la relación de campos del formulario normalizado

incluido en el Anexo III, así como para la actualización de los requisitos y criterios técnicos recogidos en el Anexo IV de este real decreto, todo ello con observancia de lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y disposiciones complementarias y en el Reglamento 1/2005, de los aspectos los accesorios de las actuaciones judiciales, aprobado por Acuerdo de 15 de septiembre de 2005 del Pleno del Consejo General del Poder Judicial.

Disposición final tercera. *Limitación del gasto público.*

El presente real decreto no supondrá incremento de gasto público ni de las dotaciones de personal.

Disposición final cuarta. *Entrada en vigor.*

El presente real decreto entrará en vigor para los órganos y oficinas judiciales y fiscales y para los profesionales de la justicia el día 1 de enero de 2016.

Para los ciudadanos que no estén representados o asistidos por profesionales de la justicia y opten por el uso de los medios electrónicos para comunicarse con la Administración de la Justicia y para aquéllos que vengan obligados a ello conforme a las leyes o reglamentos entrará en vigor el 1 de enero de 2017.

ANEXO I

Ficheros con datos de transacciones y de carácter personal en el sistema LexNET

Fichero 1. Custodia de la información acreditativa de las transacciones realizadas

a) Finalidad y usos previstos del fichero: registro, custodia y conservación segura de los documentos electrónicos acreditativos de las transacciones electrónicas.

b) Personas o colectivos titulares de los datos: los usuarios del sistema y cualquier sujeto interviniente en los procesos judiciales o actuaciones del Ministerio Fiscal.

c) Procedimiento de recogida de los datos: los datos que figuran en los resguardos electrónicos que se generan automáticamente por el sistema proceden de las relaciones de campos a cumplimentar por los usuarios.

d) Estructura básica del fichero y descripción de los tipos de datos incluidos: datos e información contenida en los resguardos electrónicos referente a la identidad del remitente y del destinatario de cada mensaje, fecha y hora de su efectiva realización proporcionada por el sistema, y proceso judicial o actuación del Ministerio Fiscal al que se refiere, indicando tipo de procedimiento, número y año, así como los escritos y notificaciones, los acuses de recibo, diligencias, recibís o cualquier otro mensaje procesal transmitido por medios electrónicos a que se refieren el apartado 2 del artículo 16 y el apartado 3 del artículo 17 de este real decreto.

e) Cesiones de datos o transferencia: no se prevén.

f) Órganos de las Administraciones responsables del fichero: Subdirección General de Nuevas Tecnologías de la Justicia. Secretaría General de la Administración de Justicia. Secretaria de Estado de Justicia. Ministerio de Justicia.

g) Servicios o unidades ante los que ejercer los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Nuevas Tecnologías de la Justicia. Secretaría General de la Administración de Justicia. Secretaria de Estado de Justicia. Ministerio de Justicia.

h) Medidas de seguridad, con indicación del nivel exigible: se adoptarán todas las medidas de seguridad correspondientes al nivel alto previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal.

Fichero 2. Gestión de usuarios del sistema LexNET

a) Finalidad y usos previstos del fichero: disponer de una relación actualizada de usuarios que tengan acceso autorizado al sistema LexNET, a efectos de la actividad de

gestión de usuarios y de establecer mecanismos o procedimientos de identificación y autenticación para dicho acceso.

b) Personas o colectivos titulares de los datos: los relacionados en el Anexo II de este real decreto.

c) Procedimiento de recogida de los datos: suministrados por el propio interesado a través de proceso de alta.

d) Estructura básica del fichero y descripción de los tipos de datos incluidos:

1.º Datos de identificación y de contacto: DNI o NIE, nombre, apellidos, dirección de correo electrónico y parte pública del certificado de usuario.

2.º Datos profesionales indicadores de la calidad de la intervención en el proceso judicial o en la actuación del Ministerio Fiscal: Cuerpo, Escala, Carrera o Colectivo profesional de pertenencia, Órgano y Unidad de destino o adscripción.

e) Cesiones de datos o transferencia: no se prevén.

f) Órganos de las Administraciones responsables del fichero: Subdirección General de Nuevas Tecnologías de la Justicia. Secretaría General de la Administración de Justicia. Secretaria de Estado de Justicia. Ministerio de Justicia.

g) Servicios o unidades ante los que ejercer los derechos de acceso, rectificación, cancelación y oposición: Subdirección General de Nuevas Tecnologías de la Justicia. Secretaría General de la Administración de Justicia. Secretaria de Estado de Justicia. Ministerio de Justicia.

h) Medidas de seguridad, con indicación del nivel exigible: se adoptarán todas las medidas de seguridad correspondientes al nivel básico previstas en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

ANEXO II

Relación de usuarios del sistema LexNET

1. Ministerio Fiscal.
2. Funcionarios del Cuerpo Superior Jurídico de Letrados de la Administración de Justicia.
3. Funcionarios de los Cuerpos de Médicos Forenses, de Facultativos del Instituto Nacional de Toxicología y Ciencias Forenses, de Técnicos Especialistas del Instituto Nacional de Toxicología y Ciencias Forenses y de Ayudantes de Laboratorio del Instituto Nacional de Toxicología y Ciencias Forenses.
4. Funcionarios del Cuerpo de Gestión Procesal y Administrativa.
5. Funcionarios del Cuerpo de Tramitación Procesal y Administrativa.
6. Funcionarios del Cuerpo de Auxilio Judicial.
7. Abogacía del Estado.
8. Ilustres Colegios de Procuradores y Procuradores.
9. Abogados.
10. Graduados Sociales.
11. Administrador del Colegio de Procuradores y, en su caso, del Colegio de Abogados.
12. Letrados de las Cortes Generales y de las Asambleas Legislativas.
13. Funcionarios y Letrados del Servicio Jurídico de la Administración de la Seguridad Social, de las demás Administraciones públicas, de las Comunidades Autónomas o de los Entes Locales.
14. Órganos de la Administración General del Estado, de las Comunidades Autónomas y de las Entidades locales y sus organismos públicos y las Fuerzas y Cuerpos de Seguridad.
15. Administradores concursales.
16. Otros que pudieran incluirse mediante la celebración del correspondiente convenio.

ANEXO III

Relación de campos a cumplimentar para la presentación de escritos a través del sistema LexNET

Campo	Observaciones
Nombre y Apellidos del remitente.	De cumplimentación automática.
Código de profesional del remitente.	De cumplimentación automática.
Nombre del Colegio profesional del remitente.	De cumplimentación automática.
Código del Colegio profesional del remitente.	De cumplimentación automática.
Nombre del órgano de destino.	Obligatorio.
Código del órgano de destino.	Obligatorio.
Tipo de procedimiento.	Obligatorio (salvo escritos iniciadores).
Número de procedimiento.	Obligatorio (salvo escritos iniciadores).
Referencia.	Texto informativo. Opcional.
Documento principal.	Obligatorio.
Documento(s) anexo(s).	Opcional
Procurador(es) destinatarios, en caso de traslado de copias.	Relación de Procuradores para seleccionar los destinatarios de las copias. Opcional.

Relación de campos a cumplimentar para la realización de actos de comunicación a través del sistema LexNET

Campo	Observaciones
Nombre del órgano remitente.	De cumplimentación automática.
Código del órgano remitente.	De cumplimentación automática.
Nombre y Apellidos del destinatario.	Obligatorio.
Código de profesional del destinatario	Obligatorio.
Nombre del Colegio profesional del destinatario.	Obligatorio.
Código del Colegio profesional del destinatario.	Obligatorio.
Tipo de procedimiento.	Obligatorio.
Número de procedimiento.	Obligatorio.
Documento principal.	Obligatorio.
Documento(s) anexo(s).	Opcional.

ANEXO IV

Requisitos de acceso y requerimientos técnicos del sistema LexNET

1. Se admitirá, a los usuarios que se relacionan en el Anexo II, la presentación de escritos y documentos y la recepción electrónica de actos de comunicación procesal mediante sistemas de identificación electrónica y de firma electrónica, según lo dispuesto en la Ley 59/2003, de 19 de diciembre, de firma electrónica, y el Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE para las transacciones electrónicas en el mercado interior.

2. Como paso previo a la utilización del sistema, los usuarios deberán solicitar el alta en el mismo con su certificado de usuario mediante la conexión a la dirección Web https://lexnet.justicia.es, salvo en aquellos casos en que la conexión pueda establecerse a través de las plataformas profesionales de los distintos operadores jurídicos reconocidas por el Ministerio de Justicia. En dicha dirección web se encontrará disponible toda la información referida a la usabilidad y accesibilidad del sistema. Esta solicitud de alta deberá ser validada por los administradores competentes de los colectivos de usuarios autorizados como garantía de pertenencia a un determinado colectivo. Sin dicha validación, el usuario no podrá utilizar el sistema.

Todo ello, sin perjuicio de las atribuciones en materia de alta de usuarios que asuman las Comunidades Autónomas que hayan recibido los traspasos de funciones y servicios en relación con los medios materiales de la Administración de Justicia en los términos de los Convenios de Cooperación Tecnológica suscritos con el Ministerio de Justicia.

3. La presentación de escritos y documentos ante los órganos y oficinas judiciales y fiscales y la recepción de los actos de comunicación que éstas cursaren, podrán ser realizadas mediante la conexión a la dirección Web https://lexnet.justicia.es; ello sin perjuicio de la posibilidad de que la conexión pueda establecerse a través de otras vías, como las plataformas profesionales, reconocidas por el Ministerio de Justicia, de los distintos operadores jurídicos, o a través de la intranet administrativa de las Administraciones públicas.

4. Cuando el uso del sistema se lleve a cabo a través de páginas web, se dará soporte a los navegadores de mayor uso entre los usuarios de LexNET.

Adicionalmente, se podrá acceder al sistema mediante servicios Web u otros mecanismos que el Ministerio de Justicia determine, basados en técnicas de interoperabilidad adecuadas con el fin de posibilitar la operatividad con otros sistemas.

5. El escrito o documento principal del envío deberá ser presentado en el formato PDF/A con la característica OCR (reconocimiento óptico de caracteres), es decir, deberá haber sido generado o escaneado con software que permita obtener como resultado final un archivo en un formato de texto editable sobre cuyo contenido puedan realizarse búsquedas y deberá ir firmado electrónicamente con la firma o firmas de los profesionales actuantes.

6. Los documentos que se adjunten a los escritos procesales, deberán ser presentados según su contenido en alguno de los formatos que la Guía de Interoperabilidad y Seguridad de Catálogo de Estándares y la Guía de Interoperabilidad y Seguridad del Documento Judicial Electrónico establezcan para este cometido. Hasta entonces se recomiendan los siguientes:.pdf,.rtf,.jpeg,.jpg,.tiff,.odt,.zip.

Los documentos que sólo contengan texto deberán ser presentados, principalmente, con las características descritas en el número anterior.

Los archivos comprimidos.zip sólo podrán contener documentos de los formatos:.pdf,.rtf,.jpeg,.jpg,.tiff,.odt.

En ningún caso se podrán remitir a través de LexNET archivos de audio, video o zip comprimido que contenga archivos en formatos distintos de los anteriormente citados.

Los documentos adjuntos deberán remitirse individualizados en tantos archivos digitales como documentos sean los que deban componer el envío. No es posible remitir un único pdf que contenga todos los documentos.

En el momento de su generación en el proceso de escaneado, los documentos serán nombrados de forma descriptiva. El nombre deberá ir precedido del número cardinal correspondiente al lugar u orden que ocuparán al ser anexados o adjuntados en el envío a realizar. Deberá incluirse su clase y breve descripción, sin que sirva únicamente una alusión genérica o numeral.

7. El sistema permitirá acceder a los archivos de forma paralela e integrada, antes de proceder al envío.

8. Los dispositivos de digitalización o escaneado que sean utilizados para la transformación en documentos digitalizados de los obrantes en papel y que se adjunte a los escritos y actos de comunicación procesales, se configurarán con las características que la Guía de Interoperabilidad y Seguridad de Digitalización establezca. Hasta su publicación se recomienda:

a) Activar la Resolución del Escáner a 200x200.ppp o, en su defecto, la mínima que permita el dispositivo.

b) Seleccionar tipo de salida de documento PDF/A.

c) Seleccionar tipo de salida: un solo documento.

d) Activar el OCR (Reconocimiento de Caracteres).

e) Seleccionar el color de Salida Negro.

Únicamente se utilizarán características de color, cuando el contenido de la información a adjuntar así lo requiera.

§ 68

Orden JUS/1126/2015, de 10 de junio, por la que se crea la sede judicial electrónica correspondiente al ámbito territorial del Ministerio de Justicia

Ministerio de Justicia
«BOE» núm. 143, de 16 de junio de 2015
Última modificación: sin modificaciones
Referencia: BOE-A-2015-6644

La Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, dedica específicamente su Título III a definir y regular la llamada «Sede Judicial Electrónica» que de conformidad con su artículo 9 se define como «aquella dirección electrónica disponible para los ciudadanos a través de redes de telecomunicaciones cuya titularidad, gestión y administración corresponde a cada una de las Administraciones competentes en materia de justicia».

Con la implantación de la Sede Judicial Electrónica se pretende centralizar los procedimientos y servicios que presta cada una de las oficinas judiciales dentro del ámbito del Ministerio de Justicia, al objeto de facilitar el acceso a las mismas, así como crear un espacio en el que la Administración de Justicia, el ciudadano y los profesionales se relacionen en el marco de la actividad judicial con las garantías procesales necesarias.

El artículo 9 del mencionado texto normativo establece que «las Administraciones competentes en materia de justicia determinarán las condiciones e instrumentos de creación de las sedes judiciales electrónicas» que en todo caso se crearán mediante disposición publicada en el «Boletín Oficial del Estado» o el «Boletín Oficial de la Comunidad Autónoma» correspondiente.

Esta Orden Ministerial ha sido informada favorablemente por el Consejo General del Poder Judicial, el Comité Técnico Estatal de la Administración de Justicia y la Agencia Española de Protección de Datos.

En consecuencia, dispongo:

Artículo 1. *Objeto.*

La presente Orden tiene por objeto la creación de la Sede Judicial Electrónica, con el fin de dar cumplimiento a lo establecido en la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

A través de la Sede Judicial Electrónica se podrán realizar todas las actuaciones, procedimientos y servicios que requieran la autenticación de la Administración de Justicia o de los ciudadanos y profesionales en sus relaciones con ésta por medios electrónicos, así como aquellas otras actuaciones respecto a las que se decida su inclusión en la sede.

Artículo 2. *Ámbito de aplicación.*

Su ámbito de aplicación se extiende a las Oficinas Judiciales que se hallen bajo la competencia del Ministerio de Justicia.

Artículo 3. *Punto de Acceso General de la Administración de Justicia.*

1. En la Sede Judicial Electrónica existirá un acceso a través del denominado Punto de Acceso General de la Administración de Justicia, a través del cual se podrá acceder a todas las sedes y subsedes judiciales electrónicas creadas dentro del territorio nacional, con independencia de la posibilidad de acceso directo a las mismas.

2. El Punto de Acceso General de la Administración de Justicia contendrá el directorio de las sedes judiciales electrónicas que, en este ámbito, faciliten el acceso a los servicios, procedimientos e informaciones accesibles correspondientes a la Administración de Justicia, al Consejo General del Poder Judicial, a la Fiscalía General del Estado y a los organismos públicos vinculados o dependientes de la misma, así como a las Administraciones con competencias en materia de Justicia. También podrá proporcionar acceso a servicios o informaciones correspondientes a otras Administraciones Públicas o corporaciones que representen los intereses de los profesionales de la justicia, mediante la celebración de los correspondientes Convenios.

3. El Punto de Acceso General de la Administración de Justicia será creado y gestionado por el Ministerio de Justicia conforme a los acuerdos que se adopten en el Comité Técnico Estatal de la Administración Judicial Electrónica, para asegurar la completa y exacta incorporación de la información y accesos publicados en éste.

Artículo 4. *Dirección electrónica de la Sede.*

La dirección electrónica de referencia de la Sede Judicial Electrónica será https://sedejudicial.justicia.es.

Artículo 5. *Titularidad y gestión de la Sede.*

a) La titularidad de la Sede Judicial Electrónica corresponderá a la Administración General del Estado.

b) La gestión tecnológica de la sede será competencia de la Secretaría General de la Administración de Justicia.

c) Serán responsables de la gestión y de los servicios puestos a disposición de los ciudadanos y profesionales en la sede judicial electrónica los órganos administrativos designados a tal efecto por el Ministerio de Justicia. Así mismo la responsabilidad de los contenidos corresponderá al órgano que origine dicha información.

Artículo 6. *Canales de acceso a los servicios disponibles en la Sede.*

Para el acceso a los servicios, actuaciones y procedimientos disponibles en la Sede Judicial Electrónica, se habilitarán los siguientes canales:

a) Para el acceso electrónico, a través de Internet.

b) Para los servicios que se ofrezcan mediante atención telefónica, los números de teléfono serán debidamente publicados en la propia sede.

Artículo 7. *Contenidos y Servicios de la Sede.*

1. Los contenidos que se prevé incorporar en esta Sede Judicial Electrónica son:

a) Identificación de la sede, así como del órgano u órganos titulares y de los responsables de la gestión, de los servicios puestos a disposición en la misma y, en su caso, de las subsedes de ella derivadas.

b) Información necesaria para la correcta utilización de la sede incluyendo el mapa de la sede judicial electrónica, con especificación de la estructura de navegación y las distintas secciones disponibles.

c) Sistema de verificación de los certificados de la Sede, que estará accesible de forma directa y gratuita.

d) Relación de sistemas de firma electrónica que sean admitidos o utilizados en la Sede Judicial Electrónica.

e) Información relacionada con la protección de datos de carácter personal, incluyendo los enlaces con la sede electrónica de la Agencia Española de Protección de Datos de Carácter Personal y los de las Agencias Autonómicas de Protección de Datos.

f) Normas de creación del Registro o Registros electrónicos accesibles desde la sede.

2. Los servicios que se prevé incorporar en la Sede Judicial Electrónica son:

a) La relación de los servicios disponibles en la sede judicial electrónica.

b) La Carta de Servicios y la Carta de Servicios Electrónicos.

c) La Carta de Derechos de los Ciudadanos ante la Justicia.

d) La relación de los medios electrónicos que los ciudadanos y profesionales pueden utilizar en cada supuesto en el ejercicio de su derecho a comunicarse con la Administración de Justicia.

e) Un enlace para la formulación de sugerencias y quejas relativas al funcionamiento de la Sede Judicial Electrónica.

f) Acceso, en los términos legalmente establecidos, al estado de tramitación del expediente.

g) Publicación electrónica, cuando proceda, de resoluciones y comunicaciones que deban publicarse en tablón de anuncios o edictos.

h) Publicación de las declaraciones de conformidad, compatibilidad y otros posibles distintivos de interoperabilidad, obtenidos respecto al cumplimiento del esquema judicial de interoperabilidad y seguridad.

i) Verificación de los sellos electrónicos de los órganos u organismos públicos que abarque la sede.

j) Comprobación de la autenticidad e integridad de los documentos emitidos por los órganos u organismos públicos que abarca la sede que hayan sido autenticados mediante código seguro de verificación.

k) Servicios de asesoramiento electrónico al usuario para la correcta utilización de la sede.

l) Puesta a disposición de los interesados de los correspondientes modelos o impresos normalizados.

3. A medida que se vayan desarrollando nuevos servicios, se incorporarán paulatinamente a la Sede.

4. Los contenidos publicados en la Sede Judicial Electrónica responderán a los criterios de publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad que se derivan de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

5. La Sede Judicial Electrónica deberá asegurar la confidencialidad, disponibilidad e integridad de las informaciones que maneja, siguiendo los criterios de seguridad que se derivan de la Ley 18/2011 de 5 de julio.

Asimismo, serán de aplicación a los datos de carácter personal que sean recogidos o tratados a través de la Sede Judicial Electrónica, las medidas de seguridad establecidas en la normativa vigente en materia de protección de datos de carácter personal.

6. La Sede Judicial Electrónica posibilitará, paulatinamente el acceso a sus contenidos y servicios en las lenguas cooficiales en el Estado español.

Artículo 8. *Medios para la formulación de sugerencias y quejas.*

El medio disponible para la formulación de sugerencias y quejas con respecto a la gestión y servicios que presta la sede, de conformidad con lo dispuesto en el artículo 9.2 de la Ley 18/2011, de 5 de julio, será la presentación telemática a través del servicio de sugerencias y quejas de la Sede Judicial Electrónica.

Artículo 9. *Sedes judiciales electrónicas derivadas.*

La Secretaría General de la Administración de Justicia, propondrá la creación de cuantas sedes judiciales electrónicas derivadas o subsedes sean necesarias en el ámbito

competencial referido en esta orden, de conformidad con los apartados 3, 4, 5 y 6 del artículo 10 de la Ley 18/2011, de 5 de julio.

La mencionada creación se llevará a cabo mediante resolución de la Secretaría de Estado de Justicia y la misma será objeto de publicación en el «Boletín Oficial del Estado».

Disposición transitoria única. *Puesta en funcionamiento de la Sede Judicial Electrónica.*

La Sede Judicial Electrónica entrará en funcionamiento dentro del plazo máximo de seis meses a contar desde la fecha de entrada en vigor de esta Orden.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Orden Ministerial.

Disposición final única. *Entrada en vigor.*

La presente Orden entrará en vigor al día siguiente de su publicación en el «Boletín Oficial del Estado».