TOMO 1

GUÍA ESTRATÉGICA EN SEGURIDAD PARA ENTIDADES LOCALES

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Cuaderno de Recomendaciones

Presentación

Ramón Fernández Pacheco Monterreal

Alcalde de Almería y Presidente de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

La Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias, que tengo el honor de presidir, tiene entre sus objetivos prioritarios contribuir a la difusión y correcto empleo de las más avanzadas técnicas, herramientas y metodologías, así como mejorar la normativa destinada a ayudar a los entes locales a desempeñar mejor, más eficazmente y conforme a la Ley, las funciones que los ciudadanos les han atribuido.

Durante 2016 esta Comisión detectó carencias en muchos de nuestros ayuntamientos respecto al cumplimiento de las directrices marcadas por el Esquema Nacional de Seguridad. Fue entonces cuando surgió la idea de trabajar en la dirección que hiciera posible paliarlas, creando un grupo de trabajo en el que, con la participación de nuestros Técnicos, pudiera darse cabida a otros actores directamente implicados tanto del ámbito público como del privado.

El objetivo del grupo sería la creación de una serie de pautas para ayudar a las Administraciones Locales a interpretar de forma práctica y homogénea las obligaciones derivadas del Esquema Nacional de Seguridad. Entre otros, algunos de los temas que se querían resolver eran:

- **la fijación de niveles de seguridad adecuadas al contexto de la Administración Local,**
- **el papel de las Diputaciones como prestadoras de servicios,**
- **la implicación que suponen paradigmas como el Cloud Computing,**
- **o, las medidas que deberán ser de aplicación para mejorar la seguridad de la información y servicios, tanto por la propia Administración Local como por los prestadores de servicio.**

Pues bien, tras el trabajo realizado en los últimos meses, por fin ve la luz el presente documento, en forma de Cuaderno de Trabajo, donde se pueden encontrar todas las claves necesarias para el cumplimiento normativo.

Estoy seguro de que este documento permitirá que cada Administración local sea capaz de elaborar su propio itinerario hacía la consecución del objetivo: Cumplir plenamente con el ENS. Por tanto, confío en la buena acogida de esta publicación y espero que su utilidad se refleje en el buen hacer del personal que trabaja para prestar un mejor servicio al ciudadano.

No me gustaría despedirme sin manifestar mi agradecimiento, como Presidente de la Comisión de Sociedad de la Información y Tecnologías, a todas las personas y/o entidades que han colaborado en este proyecto de manera absolutamente desinteresada: ¡Muchas gracias a todos por este magnífico trabajo!

Cuando se trabaja en equipo, se compagina talento y aptitudes de los miembros y se potencian los esfuerzos y el talento, disminuye el tiempo invertido en el trabajo y se mejora la eficacia de los resultados.

Para un buen trabajo en equipo es necesaria una buena comunicación, coordinación, complementariedad y sin duda éste proyecto es un buen ejemplo de ello.

Cada uno hace una parte pero todos con un objetivo común bajo el paraguas de la FEMP, que como en otras ocasiones es el mejor canal para hacer llegar este trabajo a todos los municipios de España.

Sin duda, la sinergia entre las personas que hemos participado nos acerca al éxito.
Muchas gracias por el excelente trabajo realizado.

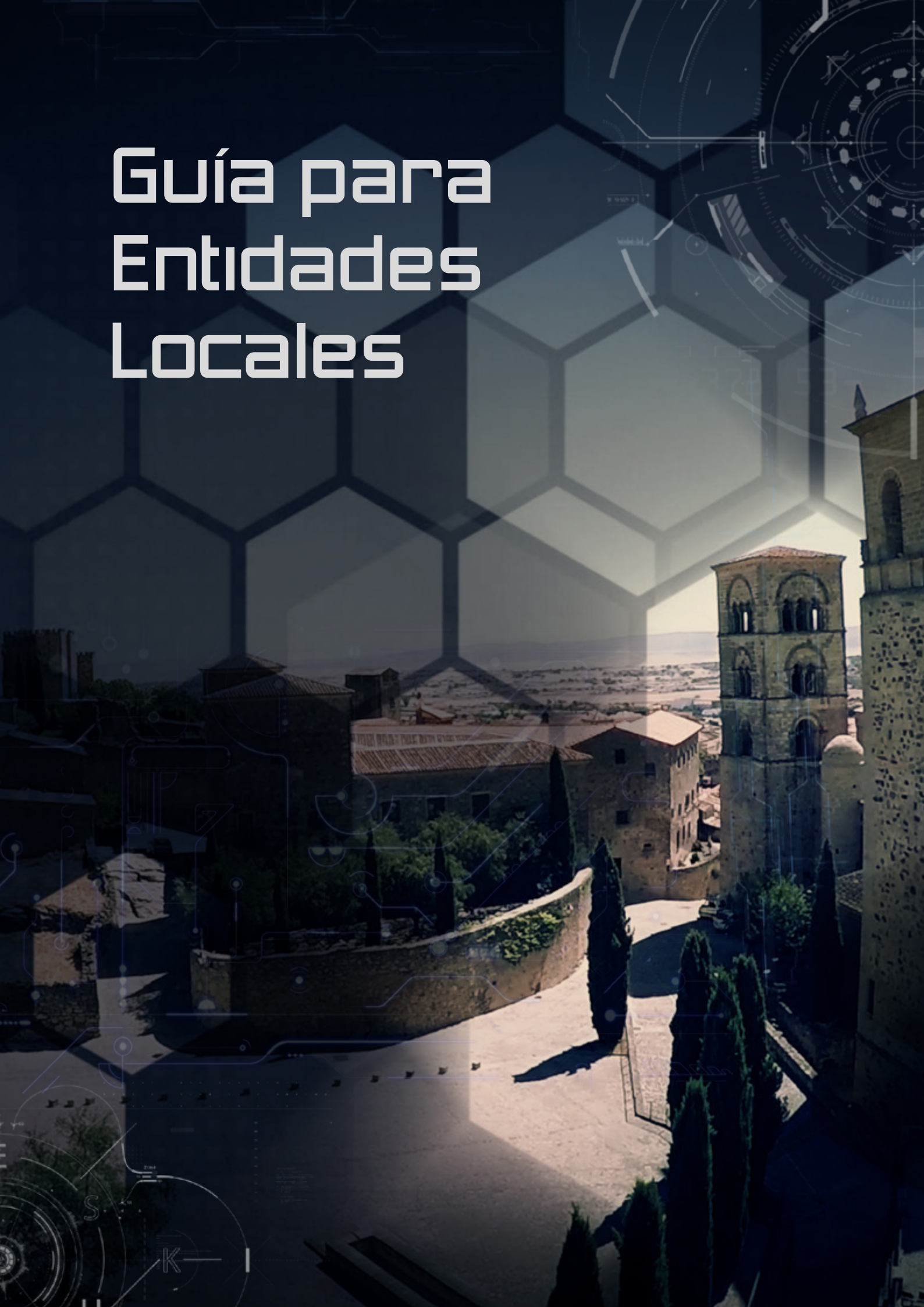
Virginia Moreno

Ayuntamiento de Leganés
Técnico de la Comisión de SSII y TT de la FEMP, Coordinadora y miembro del equipo redactor

TOMO I GUÍA PARA ENTIDADES LOCALES

ÍNDICE

Guía para Entidades Locales



CLAVES

El **alcance** del Esquema Nacional de Seguridad está determinado por las Leyes 39 /2015 y 40/2015. Resultará de aplicación a todos los sistemas de información, con independencia de que exista o no tratamiento de datos personales o que su tramitación sea a través de sede electrónica.

Los **prestadores** de servicios, públicos y privados, están dentro del alcance del ENS. Desde las Entidades Locales tenemos la obligación de exigir las Declaraciones o Certificaciones de Conformidad con el ENS, en el ámbito concreto de la prestación.

La seguridad de la organización es un proceso **Interno**, **Integral y Continuo**, **implicando a todos** los miembros de la entidad local, independientemente de su tamaño y del ámbito del sector público al que pertenezca."

Las Declaraciones o Certificaciones de Conformidad con el ENS se realizan sobre los **sistemas de información**, a diferencia de la ISO 27001 que se realiza sobre los sistemas de gestión.

La seguridad 100% no existe, es por ello que se precisa de una correcta **gestión del riesgo**, determinando tanto la probabilidad de que ocurran incidencias como de sus consecuencias.

Los Ayuntamientos de menor población deberán de apoyarse en las **Diputaciones Provinciales**, **Cabildos o Consejos Insulares** como estrategia de cumplimiento ENS.

La **Declaración o la Certificación** de conformidad con el ENS de un prestador de servicio no implica la Declaración o Certificación de la entidad Local usuaria de los servicios prestados.

En la sede electrónica del Centro Criptológico Nacional (CCN) se encuentra una relación actualizada de las únicas **Entidades de Certificación** acreditadas para expedir certificaciones de conformidad con el ENS.

El plan de adecuación que definas será tu **hoja de ruta**

La seguridad se basa en la **mejora continua**. El cumplimiento del ENS precisa la re-evaluación periódica de los sistemas de información afectados.

"La mayor inseguridad nace en la seguridad interna"
"La Falta de Seguridad complica la Transparencia"
V. Moreno

INTRODUCCIÓN

En su momento, el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, en adelante ENS, daba respuesta a los crecientes y exigentes retos sobre Seguridad. Su objeto pasa por la definición de los principios y requisitos básicos para una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información y los datos.

En el ámbito de la **transparencia y apertura de datos**, es importante destacar la importancia del factor disponibilidad de los datos, por lo que su aseguramiento puede requerir un nivel de medidas de protección mayor que el que, con carácter general, se establezca para otro tipo de informaciones o servicios.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza y seguridad en el uso de los datos y la información es, además, uno de los principios que establece la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el ENS, dejando el testigo a la nueva normativa vigente.

En todo caso, las medidas de protección deberán adaptarse tanto a los riesgos a los que esté expuesta la información y sus redes o sistemas, como a la situación tecnológica del organismo correspondiente. En el ENS, se establecen los criterios para la realización de un análisis de riesgos y las pautas a seguir para el establecimiento de unas adecuadas medidas de seguridad.

Nace el ENS con las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas e indicadores para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a la ciudadanía y a las Administraciones públicas, en adelante AA.PP, cumplir con la normativa vigente.

Con el ENS buscamos transmitir la confianza en los sistemas de información que prestarán los servicios y custodiarán la información de acuerdo con las especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Es indiscutible la seguridad de las redes y de la información, como la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los incidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Para dar cumplimiento a lo anterior se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad; se implanta la elaboración de un informe para conocer regularmente el estado de seguridad de los sistemas de información a los que se refiere el real decreto, se establece el papel de la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional, CCN-CERT, se incluye un glosario de términos y se hace una referencia expresa a la formación.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, en el ámbito de la Administración Electrónica, da cumplimiento a lo previsto en el artículo 42 Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, derogada recientemente. Su objeto pretendía establecer 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. Por tanto, la finalidad inicial del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Real Decreto 951/2015, de 23 de octubre, modifica el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, y cuya reforma tiene como objeto reforzar la protección de las Administraciones Públicas frente a las ciberamenazas mediante la adecuación a la rápida evolución de las tecnologías.

Con la entrada en vigor de 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, que recoge al ENS en su artículo 156, el marco de aplicación material **deberá de extenderse a todos los elementos vinculados con la tramitación del procedimiento administrativo**, es decir, tanto con independencia de que se presten a través de la sede electrónica (enfoque tradicional basado en la Ley 11/2007) o bien provisionados por terceros. Esta última novedad implica un importante cambio sobre el ámbito de aplicación objetivo o material (elementos sujetos), así como de su ámbito subjetivo (sujetos o entidades obligadas). Las soluciones y servicios prestados por el sector privado, comprendidos dentro del ámbito objetivo, deberán de satisfacer las exigencias legales establecidas en el mismo.

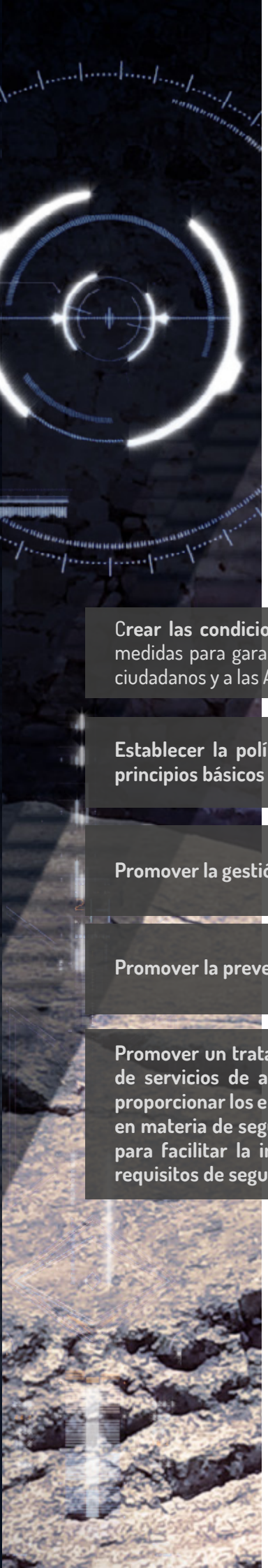
A su vez, la resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. Ello implica que la garantía de cumplimiento, **tanto en los Ayuntamientos como en los servicios prestados por el sector privado, se basará en la Declaración y Certificación de Conformidad con el ENS**, lo que implicará, para la mayoría de los sistemas[1] , someter la entidad a un proceso independiente de auditoría a través de entidades acreditadas por la ENAC, que emitirán un certificado de conformidad que deberá ser expuesto en la páginas web del Ayuntamiento o bien de las empresas del sector privado, conforme a la guía CCN-STIC-809 del Centro Criptológico Nacional.

En el siguiente enlace se pueden visualizar la lista vigente de Entidades de certificación acreditadas, o en vías de acreditación, para expedir certificaciones de conformidad con el ENS.

LA FINALIDAD INICIAL DEL ENS ES LA CREACIÓN DE LAS CONDICIONES NECESARIAS DE CONFIANZA EN EL USO DE LOS MEDIOS ELECTRÓNICOS, A TRAVÉS DE MEDIDAS PARA GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS, LOS DATOS, LAS COMUNICACIONES, Y LOS SERVICIOS ELECTRÓNICOS

[1] Los sistemas de categoría básica requieren una declaración de conformidad. Los sistemas de categoría media y alta requieren la certificación de conformidad a través de entidades acreditadas por la ENAC.

2 Objetivo y alcance



El ENS determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. Está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar la seguridad de la información en todas sus dimensiones, es decir, confidencialidad, disponibilidad, integridad, autenticidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que se gestionan las AA.PP. en el ejercicio de sus competencias.

1.1 Objetivos

El ENS persigue los siguientes objetivos:

Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las AA.PP, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Establecer la política de seguridad en la utilización de medios electrónicos constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.

Promover la gestión continuada de la seguridad, al margen de impulsos puntuales, o de su ausencia.

Promover la prevención, detección y corrección.

Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades. Esto supone proporcionar los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información; también aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.

La seguridad se concibe como una actividad integral, en la 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.

1.1.1 Elementos del Esquema Nacional de Seguridad

Los elementos principales del ENS son:

- Los **principios básicos** a considerar en las decisiones en materia de seguridad
- Los **requisitos mínimos** que permitan una protección adecuada de la información
- El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger.
- Las comunicaciones electrónicas
- La auditoría de la seguridad
- La respuesta ante incidentes de seguridad
- La certificación de la seguridad y en particular el uso de componentes evaluados y certificados
- La conformidad
- La formación y la concienciación

> El aspecto principal del ENS es, sin duda, que todos los órganos superiores de las AA.PP. deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente, que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos, según se expone a continuación...

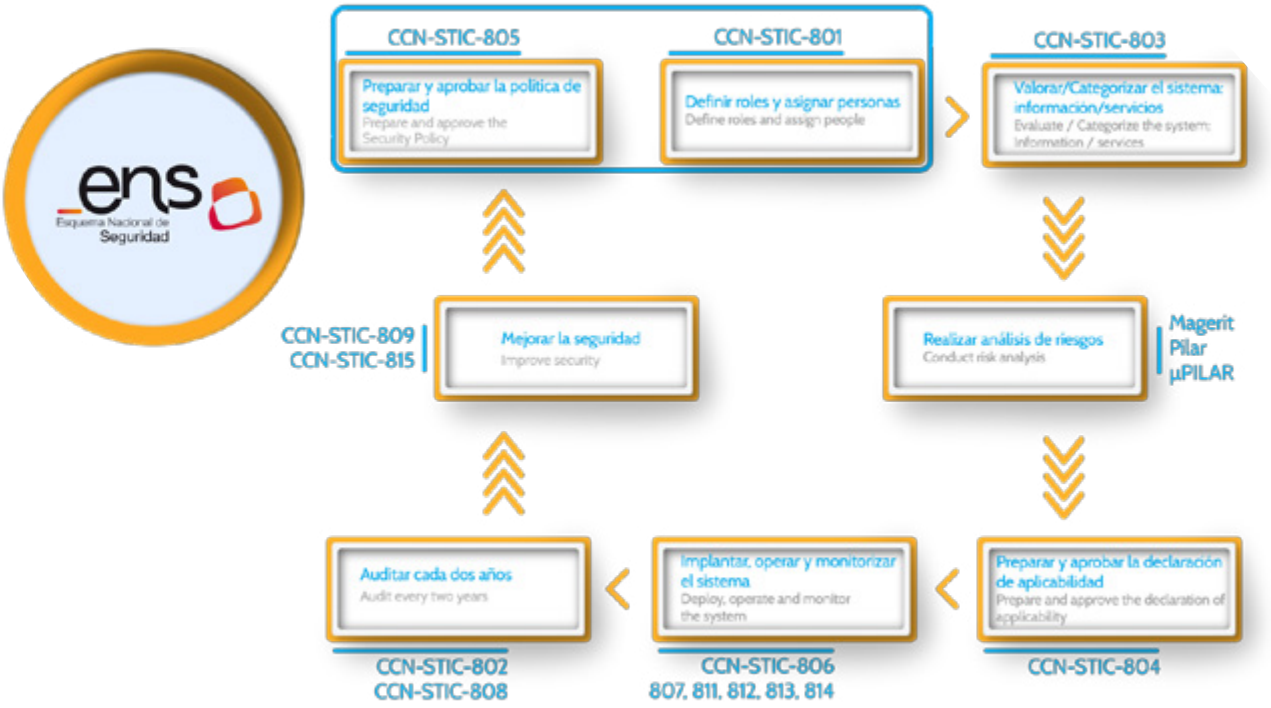
1.1.2 Adecuación al Esquema Nacional de Seguridad

En la disposición transitoria del Real Decreto 3/2010 se articulaba un mecanismo escalonado para su adecuación de manera que los sistemas de las AA.PP deberían estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación vencía el 30 de enero de 2014.

Posteriormente, 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 ENS en el ámbito de la Administración Electrónica abrió un plazo de 24 meses para la adecuación a lo previsto en la modificación que finaliza el 5 de noviembre de 2017.

La adecuación ordenada al ENS requiere el tratamiento de las siguientes cuestiones:

- Preparar y aprobar la **política de seguridad**, incluyendo la definición de roles y la asignación de responsabilidades. (Véase CCN-STIC 805 Política de seguridad de la información)
- **Categorizar los sistemas** atendiendo a la valoración de la información manejada y de los servicios prestados. (Véase CCN-STIC 803 Valoración de sistemas en el Esquema Nacional de Seguridad)
- Realizar el **análisis de riesgos**, incluyendo la valoración de las medidas de seguridad existentes. (Véase Magerit versión 3 y programas de apoyo–Pilar-)
- Preparar y aprobar la Declaración de aplicabilidad de las **medidas de seguridad** del Anexo II del ENS. (Véase CCN-STIC 804 Medidas e implantación del Esquema Nacional de Seguridad)
- Elaborar un **plan de adecuación** para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. (Véase CCN-STIC 806 Plan de adecuación del Esquema Nacional de Seguridad)
- **Implantar, operar y monitorizar** las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente. (Véase serie CCN-STIC)
- **Auditar** la seguridad (Véase CCN-STIC 802 Auditoría del Esquema Nacional de Seguridad y CCN-STIC 808 Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad).
- **Informar sobre el estado de la seguridad al órgano competente en la materia** (Véase CCN-STIC 815 Métricas e Indicadores en el Esquema Nacional de Seguridad y CCN-STIC 824 Informe del Estado de Seguridad).



1.2 Alcance

En este libro de recomendaciones sobre el itinerario para la adecuación al ENS, se habrá conseguido el objetivo principal si con la elaboración del mismo, ayudamos a saber cómo hemos de trabajar en la adecuación y medidas a adoptar dentro de nuestra organización, para asegurar la información y los datos dentro de las infraestructuras necesarias y que no se quede en una mera declaración de intenciones.

¿Para qué sirve una Guía de Recomendaciones sobre un Itinerario a seguir?

Es un plan que establece a grandes rasgos la secuencia de pasos para alcanzar un objetivo. Puede entenderse como un plan de acción a corto, medio y largo plazo, y que acerca desde los objetivos más estratégicos a objetivos más tangibles y alcanzables.

La finalidad de esta guía de recomendaciones es servir de base a la institución para saber dónde está y qué debe hacer para llegar a donde quiere llegar. Todo ello con objeto de definir sus objetivos, así como ofrecer unas líneas estratégicas claras para el desarrollo de los distintos procesos en aras de alcanzar realmente esos objetivos.

Es un plan sobre una problemática concreta a tratar, a las que hay que dar una solución.

¿Cómo se plantea la Metodología de trabajo?

El presente documento constituye el itinerario **de trabajo sobre la adecuación al ENS para las administraciones locales**.

Es un libro de trabajo sobre la adecuación al ENS dentro del proceso de Transformación Digital para las Administraciones Locales. En él se hace una descripción de las pautas, requisitos y los pasos a seguir, para conseguir definir una **hoja de ruta personalizada para la adecuación al ENS**, teniendo en cuenta la definición y marco legal del esquema, los roles a adoptar según las competencias dentro de la organización, el modelo a seguir dividido en varias fases, actuaciones, tareas y niveles así como distintos sistemas de medición , terminando en la descripción de cómo llevar a cabo la **divulgación** en el ámbito interno de la institución y hacia el exterior, acorde siempre a la nueva normativa existente para las administraciones locales.

Disponer de un libro de recomendaciones sobre el itinerario a seguir y todos los temas que hay que conocer, nos ayudará a analizar y estudiar todos los conceptos necesarios para poder abordar de forma exitosa la adecuación al ENS y cómo conseguir minimizar esa falta de seguridad en la información y los datos que generan nuestros propios sistemas y que no es fácil de solucionar.

El objetivo último es ayudar a los Ayuntamientos a definir su propia hoja de ruta personalizada de los distintos procesos de gestión que requiere la adecuación al ENS dentro del proceso global de transformación digital acorde a la nueva normativa (Ley 39/2015 de procedimiento administrativo común y Ley 40/2015 de Régimen jurídico), para las administraciones locales.

¿En qué medida me resulta de aplicación el ENS?

ENS se dirige a cualquier AA.PP.

EL OBJETIVO ÚLTIMO ES AYUDAR A LOS AYUNTAMIENTOS A DEFINIR SU PROPIA HOJA DE RUTA PERSONALIZADA DE LOS DISTINTOS PROCESOS DE GESTIÓN QUE REQUIERE LA ADECUACIÓN AL ENS DENTRO DEL PROCESO GLOBAL DE TRANSFORMACIÓN DIGITAL

2 Definición y Marco Legal

"Las Leyes 39 y 40 no serán completas
sin el cumplimiento del Esquema Nacional de Seguridad"
Carlos Galán

2.1 La seguridad de la información en el marco de la Administración electrónica

La Constitución española de 1978, en su artículo 103.1, proclama: "La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de **eficacia**, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Ley y al Derecho."

Así pues, y amparado genéricamente en el principio irrenunciable de la eficacia, el despliegue de los servicios que el Sector Público (Administraciones Públicas y Sector Público Institucional) debe prestar a los ciudadanos, especialmente cuando se usan las **Tecnologías de la Información y la Comunicación (TIC)**, exige contar –para dar cumplida respuesta a aquella exigencia constitucional– con los procedimientos administrativos, métodos y herramientas más adecuados que vengan a garantizar a todos sus destinatarios: ciudadanos y empresas, pero también el resto del Sector Público, la **seguridad y confiabilidad** de sus actos.

Efectivamente, de poco serviría poseer unas magníficas tecnologías que posibilitaran el tratamiento y la comunicación de millones de datos si los actores implicados en la vida de los procedimientos administrativos no percibieran los sistemas de información en los que se sustenta su relación como infraestructuras seguras y tan confiables como la misma esencia de sus actividades requiere.

2.2 El marco legal: de la Ley 11/2007 a las Leyes 39/2015 y 40/2015

No cabe duda –como así se ha afirmado–, que el **mejor servicio al ciudadano** constituye la razón de las **reformas** que, tras la aprobación de la Constitución, se han ido acometiendo en España para configurar una Administración moderna que haga de los **principios de eficacia y eficiencia** su razón última, y siempre con la mirada puesta en los ciudadanos y en los intereses generales.

Tal interés constituyó la principal razón de ser de la **Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos** (LAECSP, en adelante), eje vertebrador originario de la que se ha dado en llamar **Administración electrónica**, persiguiendo estar a la altura de nuestra época y del adecuado posicionamiento de nuestras Administraciones Públicas en el marco europeo e internacional. La publicación de la **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas** (LPACAP, en adelante) y la **Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público** (LRJSP, en adelante) que derogan la anterior, consolidan la primacía del uso de los medios electrónicos en el desenvolvimiento de las entidades públicas.

EL USO DE LAS TIC ACERCA LA ADMINISTRACIÓN A LOS CIUDADANOS, EMPRESAS Y PROFESIONALES

Es en ese contexto en el que el Sector Público debe comprometerse con su época y ofrecer a sus ciudadanos las **ventajas y posibilidades que la Sociedad de la Información tiene**, asumiendo su responsabilidad de contribuir a hacer realidad tal paradigma. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de aquel sector. De todo ello se derivará, a la postre, la **confianza y seguridad** que sea capaz de generar en los ciudadanos y en la bondad de la prestación de los servicios ofrecidos.

Como se ha dicho, el uso de las TIC **acerca la Administración a los ciudadanos, empresas y profesionales**. El tiempo y el espacio, en este nuevo paradigma, ya no constituyen elementos que puedan poner en peligro una comunicación adecuada -y eficaz- entre el administrado y su Administración. El uso eficiente de las TIC no sólo permite a los ciudadanos contemplar al Sector Público como una organización a su servicio y no como una burocracia pesada y exigente, sino que, además de esto, estas tecnologías facilitan el acceso a los servicios públicos a aquellas personas que antes tenían grandes dificultades para llegar a las dependencias oficiales, por motivos de localización geográfica, condiciones físicas de movilidad, etc., posibilitando la completa **integración y accesibilidad** de las personas y los grupos sociales.

> Las nuevas regulaciones, más allá de consagrar la relación con las Administraciones públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones, sitúan a los medios electrónicos en el mismo centro de la actividad pública, pasando de aquel originario podrán de la Ley 30/1992, al deberán de la Ley 11/2007 y, de éste, al son de la Ley 39/2015 y la Ley 40/2015, como elementos configuradores de una nueva realidad.

EL USO EFICIENTE DE LAS TIC FACILITAN EL ACCESO A LOS SERVICIOS PÚBLICOS POSIBILITANDO LA COMPLETA INTEGRACIÓN Y ACCESIBILIDAD DE LAS PERSONAS Y LOS GRUPOS SOCIALES

2.3 Consecuencias del derecho a la "relación electrónica".

El reconocimiento general de la relación electrónica con el Sector Público plantea varias cuestiones que es necesario contemplar:

- La progresiva utilización de medios electrónicos suscita la cuestión de la **privacidad de los datos** que se facilitan electrónicamente en relación con un expediente.
- Los legitimados tienen **derecho de acceso al estado de tramitación del procedimiento administrativo**, así como examinar los documentos de los que se compone. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe poder permitir el acceso en línea a los interesados para verificar la situación del expediente, sin mengua de todas las garantías de la privacidad.
- En todo caso, la progresiva utilización de comunicaciones electrónicas, derivada del reconocimiento del derecho a comunicarse electrónicamente con la Administración, suscita la cuestión no ya de la adaptación de ésta -recursos humanos y materiales a una nueva forma de relacionarse con los ciudadanos, sino también la cuestión de la manera de adaptar sus formas de actuación y tramitación de los expedientes y en general **racionalizar, simplificar y adaptar los procedimientos**, aprovechando la nueva realidad que imponen las TIC.
- El hecho de reconocer el derecho (obligación, en algunos casos) de los ciudadanos a comunicarse electrónicamente con la Administración plantea, en primer lugar, la necesidad de definir claramente la sede administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad.

Todo ello comporta y exige SEGURIDAD, en todas sus vertientes: administrativa, tecnológica y jurídica.

24 La Seguridad en las Leyes 39/2015 y 40/2015

Son muchos los preceptos contenidos en nuestras leyes administrativas de referencia (Ley 39/2015 y Ley 40/2015) que insisten en la necesidad de que el desenvolvimiento de las entidades del Sector Público, tanto si obedece al desarrollo del procedimiento como si responde al ejercicio general de sus competencias, debe tener lugar en el marco de un entorno que contemple todas las medidas de seguridad que sean precisas para garantizar a los administrados y a las propias entidades públicas, la integridad, confidencialidad, autenticidad y trazabilidad de la información tratada y la disponibilidad de los servicios prestados.

DEBE TENER LUGAR EN UN ENTORNO QUE CONTEMPLE TODAS LAS MEDIDAS DE SEGURIDAD QUE SEAN PRECISAS

La seguridad como proceso transversal

La Ley 39/2015 recoge entre los derechos de las personas en sus relaciones con las Administraciones Públicas, 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"*. Realiza, además, diversas menciones al cumplimiento de las garantías y medidas de seguridad al referirse a registros, archivo de documentos y copias.

La Ley 40/2015, por su parte, recoge en su artículo 156 el Esquema Nacional de Seguridad, así mismo menciona la seguridad al referirse a las relaciones de las administraciones por medios electrónicos, la sede electrónica, el archivo electrónico de documentos, los intercambios electrónicos en entornos cerrados de comunicaciones y las transmisiones de datos entre Administraciones Públicas.

Algunos ejemplos de preceptos contenidos en el citado ordenamiento que refuerzan la necesidad de "seguridad" se muestran seguidamente.

Ley 39/2015 – Procedimiento Administrativo Común de las AA.PP.

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

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.

Art. 16. Registro

1... 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.

Art. 17. Archivo de documentos

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, 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.

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

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 ENS y sus normas técnicas de desarrollo.

Art. 28. Documentos aportados por los interesados al procedimiento administrativo.

3... Se presumirá que esta consulta es autorizada por los interesados, salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso, debiendo, en ambos casos, ser informados previamente de sus derechos en materia de protección de datos de carácter personal.

Art. 31 Cómputo de plazos en los registros

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

Art. 40. Notificación

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.

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

.. 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 ENS, y sus normas técnicas de desarrollo.

Ley 40/2015 – Régimen Jurídico del Sector Público

Art. 38. Sede electrónica

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.
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.

Art. 44. Intercambio electrónico de datos en entornos cerrados de comunicación

4. En todo caso deberá garantizarse la **seguridad** del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Art. 46. Archivo electrónico de documentos

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, 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

Art. 155. Transmisiones de datos entre Administraciones Públicas.

1. De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal 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.

LOS MEDIOS O SOPORTES DEBERÁN CONTAR CON MEDIDAS QUE GARANTICEN LA INTEGRIDAD, AUTENTICIDAD, CONFIDENCIALIDAD, CALIDAD, PROTECCIÓN Y CONSERVACIÓN DE LOS DOCUMENTOS ALMACENADOS

2.5 ¿Qué es el Esquema Nacional de Seguridad? Un enfoque legal

Regulado en el Real Decreto 3/2010, de 8 de enero, actualizado mediante Real Decreto 951/2015, de 23 de octubre.

Como hemos dicho y así se señala en el texto introductorio a la norma, en el ámbito de las Administraciones Públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello vino a dar respuesta, primero, el artículo 42.2 de la derogada LAECSP y, actualmente, el artículo 156.2 de la LRJSP, mediante la creación del ENS, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

Así, y por la parte que ahora nos interesa, el citado artículo 156, señala:

> **Artículo 156. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.**
>
> 1...
> *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.*

Llegado este punto, hay que decir que el ENS define Política de Seguridad como:

> *"Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos."*

Y que la definición que hace de Sistema de Información es:

> *"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."*

El ENS, desarrollando el mandato del artículo 156.2 de la LRJSP (y, antes, del artículo 42.2 de la LAECSP), contiene:

Los Principios Básicos y los Requisitos Mínimos para alcanzar la antedicha protección de la información.

Atendiendo a las siguientes definiciones:

Principios Básicos de Seguridad

"Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios."

Requisitos Mínimos de Seguridad

"Exigencias necesarias para asegurar la información y los servicios."

Tales Principios Básicos y Requisitos Mínimos serán aplicados obligatoriamente por todas las entidades del sector Público para asegurar el **acceso**, la **integridad**, la **disponibilidad**, la **autenticidad**, la **confidencialidad**, **la trazabilidad** y la **conservación** de los datos, informaciones y servicios que traten o manejen tales entidades.

La finalidad del ENS

Es la **creación de las condiciones necesarias de confianza** en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitan a los ciudadanos y a las entidades de las Administraciones públicas y el Sector Público Institucional el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En definitiva, el ENS persigue fundamentar la confianza de que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas, desarrollándose y perfeccionándose en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Por otro lado, en la actualidad, los sistemas de información de las Administraciones Públicas no constituyen elementos aislados, sino que, por el contrario, suelen estar **poderosamente interconectados**, pudiéndose conectar también con otros sistemas pertenecientes al resto del sector público, el sector privado, ciudadanos, profesionales y empresas.

Por tanto, ante la multiplicidad de amenazas que pueden poner en peligro las referidas relaciones electrónicas, se hace necesario dotar a las redes y a los sistemas de información de la necesaria **Seguridad de la Información**: **la Ciberseguridad**, a la que podemos definir como:

La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

2.6 Las Instrucciones Técnicas de Seguridad del ENS

Tal y como prescribe el artículo 29 del ENS, el **Ministerio de Hacienda y Función Pública**, a propuesta de la Comisión Sectorial de Administración Electrónica, y a iniciativa del **Centro Criptológico Nacional (CCN)**, aprobará las Instrucciones Técnicas de Seguridad, de obligado cumplimiento, y se publicarán mediante resolución de la Secretaría de Estado de Función Pública, siendo esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así, estas **Instrucciones Técnicas de Seguridad (ITS)**, que la Disposición Adicional cuarta del ENS recoge en una primera lista no exhaustiva, 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 ENS;
- Adquisición de Productos de Seguridad;
- Criptología de empleo en el ENS;
- Interconexión en el ENS y
- Requisitos de Seguridad en entornos externalizados;

Sin perjuicio, como se indicaba, de las propuestas que pueda acordar la Comisión Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29[2].

2.7 Ámbito de aplicación del ENS

De manera análoga a lo que sucede con buena parte del ordenamiento jurídico, el ámbito de aplicación del ENS es doble, a saber:

Por razón de los sujetos o entidades a los que se dirige la norma.	**ÁMBITO SUBJETIVO DE APLICACIÓN**
Por razón de las materias que son objeto de su regulación.	**ÁMBITO OBJETIVO o MATERIAL DE APLICACIÓN**

[2] A la fecha de redacción del presente texto, las ITS publicadas son: 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 y 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 (ambas en el BOE Núm. 265, Miércoles 2 de noviembre de 2016).

Ámbito subjetivo de aplicación

El ENS será aplicado a los sistemas de información del Sector Público para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestione en el ejercicio de sus competencias.

Tras la entrada en vigor de la LRJSP, el ámbito subjetivo de aplicación del ENS se determina atendiendo a lo recogido en el apartado segundo del artículo 156 de aquella norma, que señala:

> *"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".*

Por su parte, el ámbito subjetivo de aplicación de la LRJSP está definido en su artículo 2, que señala:

"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.

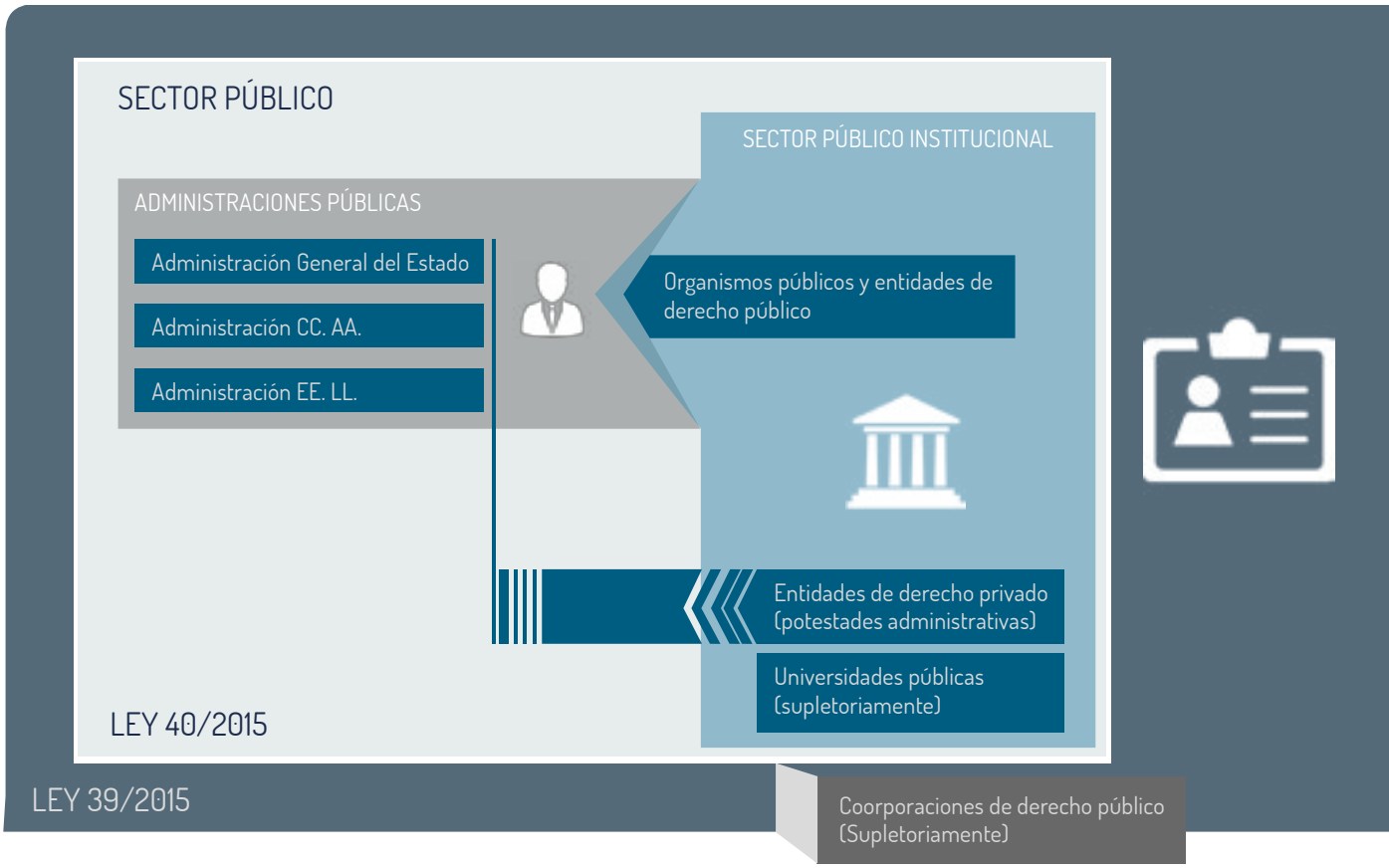
c) Las Universidades públicas que se regirán por su normativa específica y supletoriamente por las previsiones de la presente Ley.

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."

Por otro lado, y como quiera que las medidas de seguridad contempladas en el ENS no son sólo exigibles a las relaciones ad intra (relaciones entre entidades o Administraciones Públicas)[3], sino que deben extenderse también a las relaciones ad extra (relaciones entre las Administraciones y los ciudadanos), este ámbito de aplicación debe completarse con el recogido en la Ley 39/2015, y que añade al anterior el siguiente párrafo:

> *"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."*

La figura siguiente muestra un esquema del ámbito subjetivo de aplicación del ENS, en base a los respectivos ámbitos de aplicación de la LPACAP y la LRJSP[4].



Ámbito subjetivo de aplicación del ENS

[3] La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, contiene significativas referencias a la aplicación del Esquema Nacional de Seguridad y, en general, a la seguridad de la información, tales como las realizadas en el art. 13 (Derechos de las personas en sus relaciones con las Administraciones Públicas), art. 16 (Registros), art. 17 (Archivo de documentos), art. 27(Validez y eficacia de las copias realizadas por las Administraciones Públicas), art. 31 (Cómputo de plazos en los registros), art. 56 (Medidas provisionales), Disposición Adicional Segunda (Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado).

[4] Fuente: Guía CCN-STIC 830 Ámbito de aplicación del ENS.

Por todo lo anterior, el ENS es de aplicación a las entidades que conforman las denominadas **Administraciones Públicas** (AGE, CC.AA., EE.LL. y organismos públicos y entidades de derecho público vinculados o dependientes de las anteriores) y también a las **entidades de derecho privado vinculadas o dependientes de ellas**, cuando ejerzan potestades administrativas por atribución directa o delegación, de acuerdo a la legislación autonómica aplicable, así como en cuanto a su régimen de patrimonio y en materia de responsabilidad patrimonial ante terceros por el funcionamiento de sus servicios, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas en los términos establecidos por esta.

Por su parte, el ENS será de aplicación a las entidades de derecho privado vinculadas o dependientes de la Administración de las **Entidades Locales** en las materias en que les sea de aplicación la normativa presupuestaria, contable, de control financiero, de control de eficacia y contratación, de acuerdo a lo dispuesto por la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, así como en el ejercicio de las funciones públicas que les hayan sido atribuidas estatutariamente, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas en los términos establecidos por esta. Asimismo, el ENS será de aplicación a las **Universidades** de forma supletoria, es decir, en todo aquello que su propia normativa no entre a regular.

Además, el ENS será de aplicación a las **Corporaciones de Derecho Público** en el ejercicio de las funciones públicas que les hayan sido atribuidas por Ley o delegadas por una Administración Pública, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, en los términos establecidos por esta, de forma supletoria a su normativa específica.

Finalmente, y por lo que respecta a las **Fundaciones**, están comprendidas dentro del sector público las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas en la medida que están sujetas a las normas de la Ley de Régimen Jurídico del Sector Público que específicamente se refieran a las mismas y, en todo caso, cuando ejerzan potestades administrativas. Las fundaciones, tanto las privadas como las del sector público estatal, tienen personalidad jurídica privada y, por tanto, también les resulta de aplicación en los mismos casos indicados en los apartados anteriores.

Ámbito objetivo o material de aplicación

La primera y más amplia referencia al ámbito de aplicación objetivo o material del ENS (sistemas de información a los que les es de aplicación) se encuentra en el número dos de su artículo 1, cuando señala:

> *"2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas 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."*

Este párrafo contiene dos cuestiones que conviene comentar:

1. La aplicación del ENS (que el párrafo encomienda a las "Administraciones Públicas"), habrá que entenderlo hecho al ámbito subjetivo definido anteriormente, trayendo causa de lo dispuesto en las leyes 39/2015 y 40/2015.

2. El objeto último de la protección perseguida por el ENS es muy claro, cuando señala: "... 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."

Por tanto, y siempre que esté sustentado en medios electrónicos y sea responsabilidad última de una entidad pública del ámbito subjetivo de aplicación, bastará que el sistema de información en cuestión se dirija a gestionar las competencias de la entidad pública correspondiente para que le sea de aplicación el ENS[5].

Sobre este particular, conviene señalar que el concepto "**sistema de información**" es muy amplio y que, atendiendo a lo señalado en UNE-ISO/IEC 27000:2014, podemos definirlo como:

"Conjunto de aplicaciones, servicios, activos relacionados con tecnologías de la información y otros componentes para manejar información".

Por consiguiente, partiendo de que el mandato legal del ENS lo constituye esencialmente la protección de la información tratada y los servicios prestados, conviene recordar que el ENS debe aplicarse técnicamente **a todos los elementos** que, en relación con tales informaciones o servicios, puedan ser directa o indirectamente atacados. Estos elementos se detallan en el Anexo II del ENS (hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros).

Finalmente, y atendiendo a la **exigencia de desenvolvimiento electrónico** que prescriben las leyes LPACAP y LRJSP, el marco de aplicación material señalado en el párrafo anterior se concretará en todas y cada una de las actuaciones de las entidades públicas del ámbito subjetivo de aplicación del ENS **que desarrollen o contribuyan a desarrollar el procedimiento administrativo**.

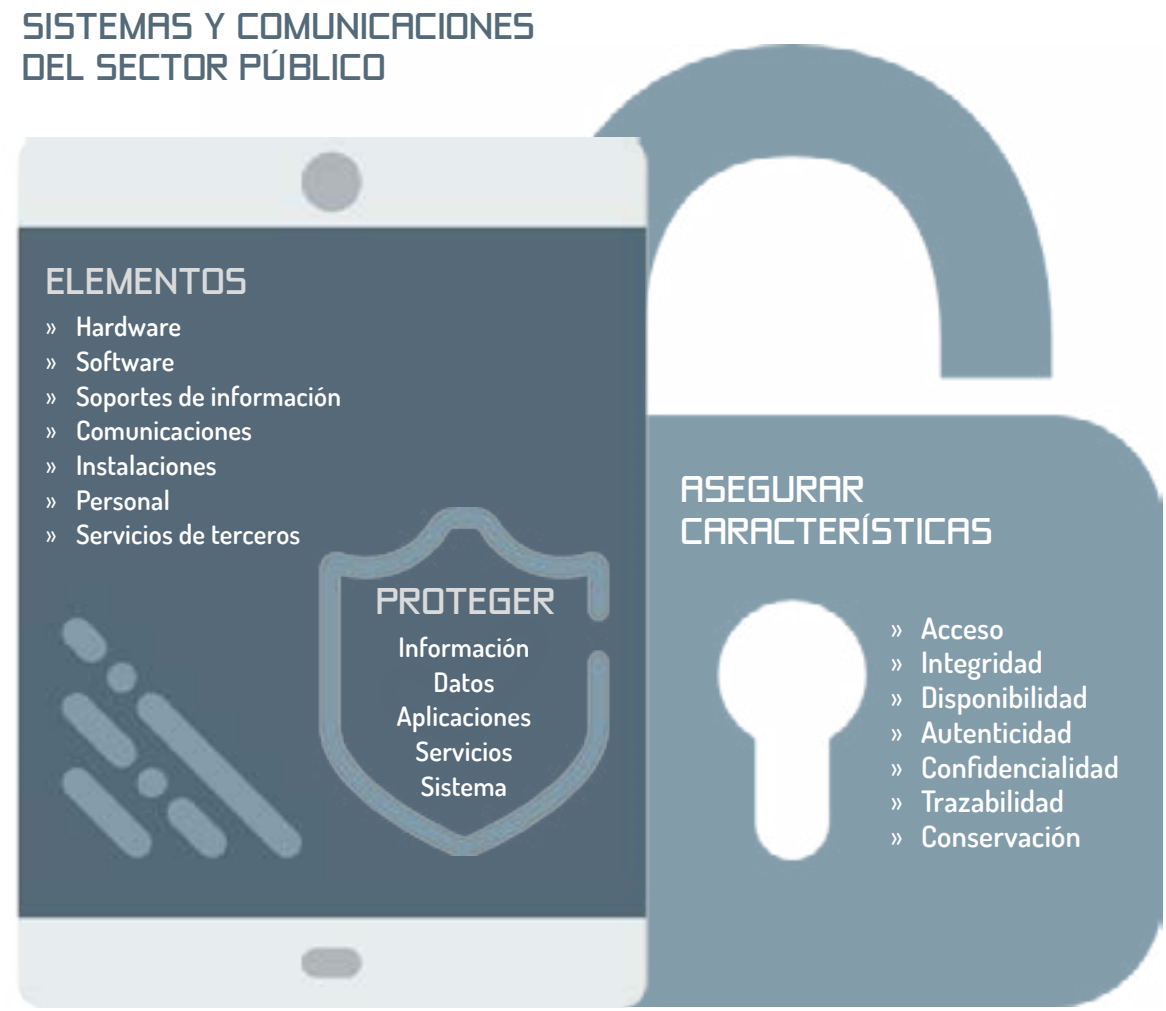
Así pues, entre otras, el ENS será de aplicación a todo lo relativo a:

- Facilitar, por medios electrónicos, el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones públicas.
- Facilitar, por medios electrónicos, los derechos de los ciudadanos, en su calidad de interesados en el Procedimiento Administrativo (arts. 13, 28, 53 y 66.1b de la LPACAP).
- Facilitar el uso de los medios de identificación y firma electrónica de los interesados en el procedimiento administrativo, incluyendo su representación y los registros electrónicos de apoderamientos (arts. 9-11, 5 y 6 LRJSP).
- Facilitar, por medios electrónicos, el derecho de los interesados a ser asistidos en el uso de los medios electrónicos en sus relaciones con las AA.PP. (arts. 12 y 13 LPACAP).
- Facilitar a los ciudadanos, por medios electrónicos, el derecho de información (arts. 21.4, 27.3 y DA4 LPACAP).
- Los Registros electrónicos (art. 16 LPACAP).
- El Archivo electrónico de documentos y expedientes (art. 17 LPACAP).

[5] Obviamente, dejando fuera los sistemas que tratan información clasificada, como prescribe el propio art. 3 del ENS o la capacidad de exclusión señalada en el art. 30 del ENS, que habrá que entenderla referida siempre a sistemas que no estuvieren dedicados a gestionar las funciones o competencias propias de la entidad pública de que se trate.

- La tramitación electrónica de los procedimientos, incluyendo el cómputo de plazos, la notificación electrónica, la gestión electrónica de expedientes y la tramitación electrónica del procedimiento, en general (arts. 30, 41-43, 70 y Título IV de la LPACAP).
- La relación, por medios electrónicos, entre las propias entidades de las AA.PP., sus órganos, organismos públicos y entidades vinculadas o dependientes (art. 3 LRJSP).
- El funcionamiento electrónico de la Administración, incluyendo las sedes electrónicas y los portales de Internet, los sistemas de identificación y firma, y la actuación administrativa automatizada, el intercambio electrónico de datos en entornos cerrados, el aseguramiento de la interoperabilidad de la firma electrónica y el archivo electrónico de documentos (arts. 38, 39, 40-43, 44, 45 y 46 de la LRJSP).
- Las relaciones electrónicas entre las Administraciones, incluyendo las transmisiones de datos entre AA.PP., los ENI y ENS, la reutilización de sistemas y aplicaciones y la transferencia de tecnologías (arts. 155, 156, 157 y 158 de la LRJSP).

La figura siguiente muestra, esquemáticamente, un ejemplo del alcance del ámbito material de aplicación del ENS.



ÁMBITO OBJETIVO DE APLICACIÓN DEL ENS

Ejemplos de sistemas y comunicaciones del Sector Público:

- Archivo electrónico de procedimientos administrativos
- Registros electrónicos
- Procedimientos electrónicos
- Padrón municipal
- Gestión de citas
- Gestión de vacantes de un Hospital
- Gestión de expedientes académicos
- Perfil del contratante
- Gestión de Recursos Humanos
- Contabilidad
- Gestión tributaria

Los servicios prestados por terceros

Los servicios comprendidos dentro del ámbito objetivo de aplicación del ENS, cuando sean suministrados o prestados por terceros (organizaciones públicas o privadas), habrán de satisfacer igualmente las exigencias legales establecidas en el mismo.

Por ello, las entidades a las que se destinan las soluciones o sean titulares de los servicios prestados, indicados en el epígrafe anterior, **exigirán a tales terceros la conformidad con el ENS de sus servicios**, en los términos establecidos en la Declaración o Certificación de Conformidad con el ENS.

La Guía CCN-STIC-809 Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento" reco gidos en la ***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 ENS***.

El Ayuntamiento deberá requerir soluciones y servicios seguros

Será responsabilidad de las entidades receptoras de las soluciones o titulares de los servicios prestados, exigir a las empresas que suministren las soluciones o presten el servicio, la obligación de que estas soluciones o servicios sean conformes con lo dispuesto en el ENS y posean las correspondientes Declaraciones o Certificaciones de Conformidad según lo señalado en la antedicha Instrucción Técnica de Seguridad.

2.8 La conexión entre el ENS y el Reglamento General de Protección de Datos

Las Entidades Locales vienen actuando como Responsables y/o Encargados de Tratamiento de datos personales en el desarrollo de buena parte de sus actividades. Por este motivo, tales entidades se van a ver afectadas por las previsiones del nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea[6], publicado en mayo de 2016 y que será de plena aplicación a partir del 25 de mayo de 2018, lo que exige que las modificaciones que deberán realizarse para alinear la normativa y la práctica de las Entidades Locales con las previsiones del RGPD habrán de estar listas para esa fecha.

En tal sentido, la Agencia Española de Protección de Datos ha señalado[7] la necesidad de acometer las actividades que se muestran seguidamente.

	Exigencia	Comentario adicional
1	La Entidad Local debe identificar con precisión las **finalidades y la base jurídica** de los tratamientos que se llevan a cabo en las Entidades Locales.	Las finalidades o la base jurídica de los tratamientos son informaciones que deben proporcionarse a los interesados (arts. 13 y 14 RGPD) y recogerse en el registro de actividades de tratamiento.
2	Cuando el tratamiento realizado por la Entidad Local persiga el cumplimiento de una tarea en **interés público** o el ejercicio de poder públicos, es necesario que el interés público como los poderes públicos que justifican el tratamiento deben **estar establecidos en una norma de rango legal**.	
3	Cuando la base jurídica de los tratamientos sea el **consentimiento** (del vecino del municipio de que se trate, por ejemplo), tal consentimiento debe ser **informado**, **libre**, **específico** y otorgado por los interesados mediante una manifestación que muestre su **voluntad de consentir** o mediante una clara acción afirmativa.	Los consentimientos conocidos como "tácitos", basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad.
4	Debe **adecuarse la información que se ofrece** a los interesados a las exigencias del RGPD (arts. 13 y 14), cuando la Entidad Local recaba sus datos.	El RGPD obliga a ofrecer una información que es más amplia que la actualmente exigida por la Ley Orgánica de Protección de Datos. Obliga, además, a que esta información se proporcione de forma "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo".
5	La Entidad Local debe establecer **mecanismos visibles, accesibles y sencillos**, incluidos los medios electrónicos, para el **ejercicio de derechos**.	Estos mecanismos deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.

[6] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES
[7] Fuente: AEPD "EL impacto del RGPD sobre la actividad de las AA.PP."

	Exigencia	Comentario adicional
6	La Entidad Local debe establecer procedimientos que permitan **responder a los ejercicios de derechos** en los plazos previstos por el RGPD.	En algunos casos será preciso valorar la necesidad de que sean los Encargados del Tratamiento con los que la Entidad Local haya contratado la prestación de determinados servicios los que colaboren en la atención a las solicitudes de los interesados.
7	La Entidad Local debe **valorar si los encargados** con los que haya contratado (o vaya a contratar) operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD.	El RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente a aquellos que estén en condiciones cumplir con el RGPD.
8	La Entidad Local debe **adecuar los contratos de encargo** que actualmente tengan suscritos a las previsiones del RGPD.	El RGPD exige expresamente que tanto los contratos como los actos jurídicos deberán tener un contenido mínimo que excede del actualmente previsto por la normativa española de protección de datos.
9	Es necesario que la Entidad Local desarrolle un **análisis del riesgo** para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se acometan.	En el contexto de las AAPP se dispone de metodologías de análisis de riesgos[8] focalizadas principalmente en la seguridad de la información, que deberán ampliarse para incluir riesgos asociados al incumplimiento de las disposiciones del RGPD.
10	La Entidad Local debe establecer un **Registro de Actividades de Tratamiento**.	El RGPD establece un contenido mínimo de ese Registro, que deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.
11	La Entidad Local debe **revisar las medidas de seguridad** que se aplican a los tratamientos, a la luz de los resultados del análisis de riesgo de los mismos.	El RGPD deja sin efecto las previsiones del RD 1720/2007, en la medida en que exige que las medidas de seguridad se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes. En el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el ENS.
12	La Entidad Local debe establecer mecanismos para **identificar** con rapidez la existencia de **violaciones de seguridad de los datos** y reaccionar ante ellas.	Para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados.

[8] Metodología MAGERIT, para la que se dispone de las herramientas PILAR, descargables en la página web del (CCN-CERT).

	Exigencia	Comentario adicional
13	Necesidad de valorar si los tratamientos que se realizan en la Entidad Local requieren una **Evaluación de Impacto** sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y de disponer de una metodología para llevarla a cabo.	El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo. También contempla un contenido mínimo de las Evaluaciones de Impacto.
14	Necesidad de designar un **Delegado de Protección de Datos** (DPD/DPO) en todas las "autoridades u organismos públicos".	El RGPD establece cuáles habrán de ser los criterios para la designación de los DPD/DPO, su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.
15	Necesidad de adaptar los instrumentos de **transferencia internacional de datos** personales a las previsiones del RGPD.	El RGPD mantiene el modelo de transferencias internacionales ya existente, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que no requerirán de autorización previa de las autoridades de protección de datos.

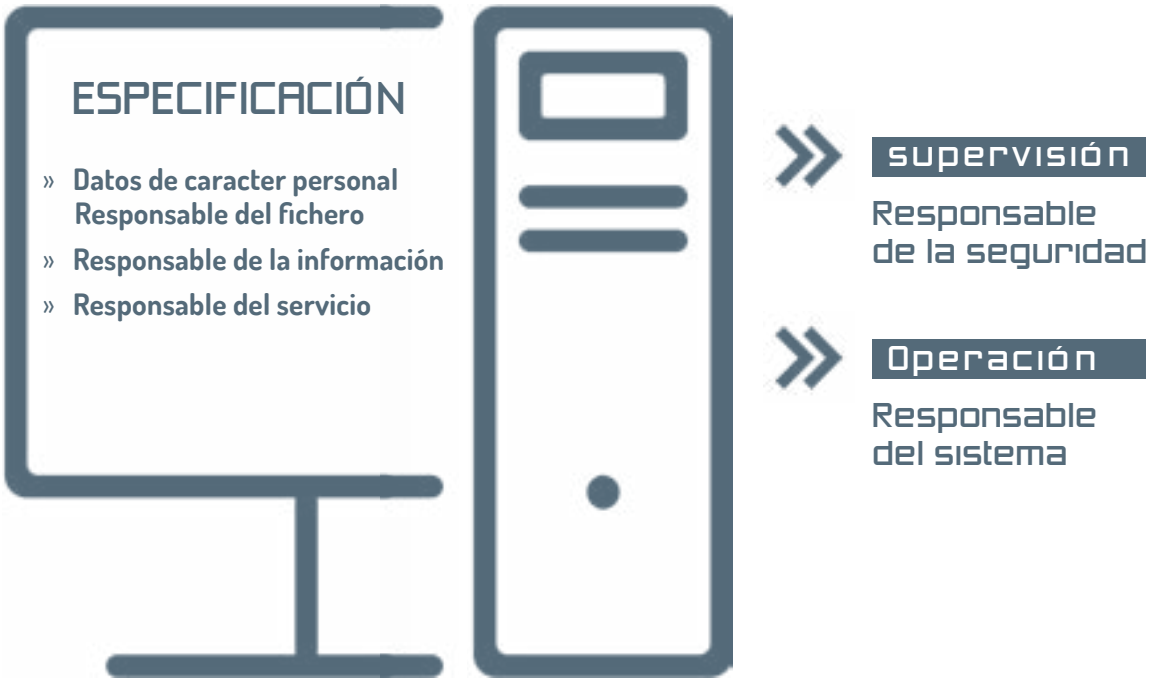
Obsérvese en el cuadro anterior, la presencia del ENS en el punto 9 (de forma implícita) y en el punto 11 (de forma explícita).

ES NECESARIO DESIGNAR UN DELEGADO DE PROTECCIÓN DE DATOS (DPD/DPO) EN TODAS LAS "AUTORIDADES U ORGANISMOS PÚBLICOS"

2.9 Principales roles

2.9.1 Las responsabilidades en la seguridad de la información

En virtud de lo dispuesto en el ENS, y con el objetivo situado en garantizar la seguridad de la información tratada y los servicios prestados, aparecen distintas figuras, atendiendo a la responsabilidad que tienen en la **especificación**, **supervisión y operación** de la seguridad de la información de la entidad.



Como se muestra en la figura anterior, los actores principales son: el Responsable de la Información, el Responsable del Servicio, el Responsable de la Seguridad, el Responsable del Sistema, y cuyas funciones esenciales son la siguientes:

- El **Responsable de la Información** determinará los requisitos de la información tratada.
- El **Responsable del Servicio** determinará los requisitos de los servicios prestados, y
- El **Responsable de Seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- El **Responsable del Sistema** es el encargado de la explotación tecnológica de la información tratada y los servicios prestados.

Seguidamente se recogen las definiciones que, de tales responsables, hace la Guía-STIC-801, del CCN.

2.9.2 Responsable de la Información

Es la persona (u órgano colegiado dentro de la entidad local de que se trate) que tiene la potestad de establecer los requisitos de la información en materia de seguridad. Esto es, la persona que **determina los niveles de seguridad de la información**.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

Como se ha dicho en capítulos precedentes, la determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del ENS. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

En las entidades locales, por lo general, el Responsable de la Información es un alto directivo de la misma, desde el punto de vista político (Alcalde, por ejemplo) o institucional (Secretario General, por ejemplo).

2.9.3 Responsable del Servicio

Es la persona (u órgano colegiado de la entidad de que se trate) que tiene la potestad de establecer los requisitos del servicio en materia de seguridad. Esto es, la persona que determina los **niveles de seguridad de los servicios**.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

Como en el caso anterior, la determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del ENS. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

Análogamente, en las entidades locales, por lo general, el Responsable del servicio es un alto directivo de la misma, desde el punto de vista político (Alcalde, por ejemplo) o institucional (Secretario General, por ejemplo).

Así pues, es posible que, en el seno de una entidad local, coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. No obstante, la diferenciación tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

2.9.4 Responsable de Seguridad

Es la persona designada por la entidad local, según procedimiento descrito en su Política de Seguridad, pudiendo ser una persona o un órgano colegiado (Comité, en la terminología habitual) y cuyas funciones son:

1. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
2. Realizar o promover las autoevaluaciones o auditorías periódicas que permitan verificar el cumplimiento del ENS.
3. Promover la formación y concienciación STIC dentro de su ámbito de responsabilidad.
4. Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
5. Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
6. Monitorizar el estado de seguridad del sistema, que podrá ser proporcionado por elementos específicos, tales como herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
7. Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
8. Elaborar el informe periódico de seguridad para la alta dirección de la entidad local, incluyendo los incidentes más relevantes del periodo.

Una cuestión importante:

Aunque el ENS señala que la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, esta exigencia puede resultar de difícil o imposible cumplimiento en corporaciones locales de tamaño reducido, donde los recursos humanos son muy limitados y donde, en consecuencia, una misma persona podría desempeñar ambas responsabilidades.

La Política de Seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

2.9.5 Otros actores

Además de los anteriores, cuando la dimensión de la entidad local lo posibilite y la magnitud de la información tratada o los servicios prestados así lo aconseje, cabe la existencia de algún otro rol personal, como los señalados seguidamente.

Responsable de Sistemas Delegados (RSD)

Cuando en un sistema de información, por razón de su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada Organización podrá designar **Responsables de Sistema Delegados (RSD)**.

Las funciones de estos RSD serán aquellas que le hayan sido delegadas por el Responsable del Sistema, y estarán relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información.

Cada RSD mantendrá tendrá una dependencia funcional directa del Responsable del Sistema, que es quién tiene la responsabilidad sobre la totalidad del sistema.

Administrador de la Seguridad del Sistema (ASS):

Designada por el propietario del sistema a propuesta del Responsable del Sistema, tiene las siguientes funciones:

- La elaboración, cuando así lo determine el Responsable del Sistema, aplicación y gestión de los Procedimientos Operativos de Seguridad.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema.
- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema.
- Informar a los Responsable de Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Aprobar los procedimientos locales de control de cambios en la configuración vigente del Sistema.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejo del sistema.
- Asegurar que la trazabilidad, auditoría y otros registros de seguridad se llevan a cabo frecuentemente, de acuerdo con la política de seguridad establecida por la Organización.
- Establecer procedimientos de seguimiento y reacción ante alarmas y situaciones imprevistas.
- Iniciar el proceso de respuesta ante incidentes que se produzcan en el Sistema bajo su responsabilidad, informando y colaborando con el Responsable de Seguridad en la investigación de los mismos.

Finalmente, en emplazamientos donde se encuentren ubicados varios sistemas de información, las funciones de ASS de cada uno de ellos podrían recaer en la misma persona.

Administrador del Sistema

Realiza las tareas de administración del sistema, coordinando a los operadores del Sistema.

Administrador de Red

Se encarga de las tareas de administración de red, siendo responsable de aspectos de seguridad relativos a la infraestructura de red (enrutadores/switches, dispositivos de protección de perímetro, redes privadas virtuales, detección de intrusión, etc.)

Operadores del Sistema

Son responsables de la operación diaria de los servicios del sistema de información. Son los primeros receptores de las incidencias que se produzcan, notificadas por los usuarios. Resolverán los incidentes que por procedimiento les competan y elevarán al Administrador de Seguridad (ASS) correspondiente las que les excedan.

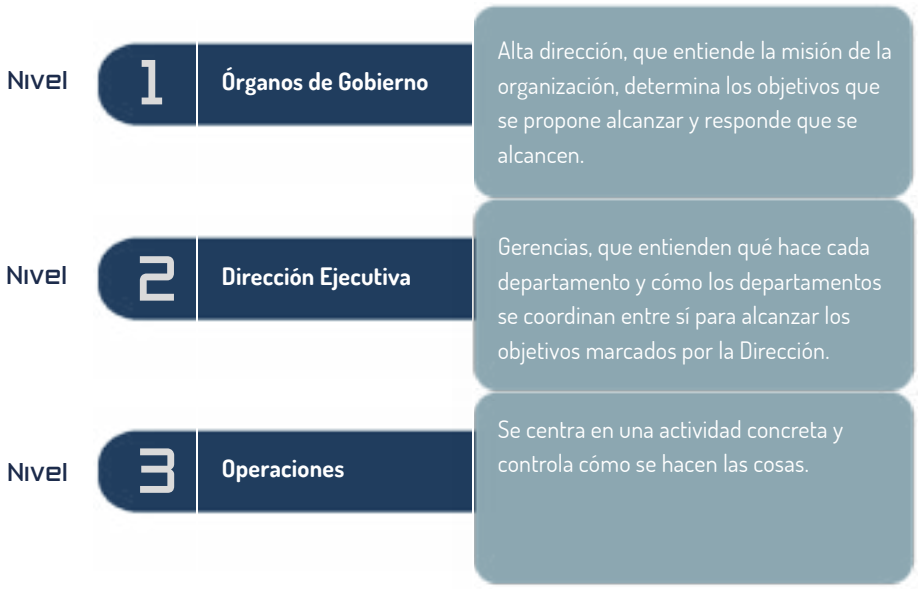
Usuarios del Sistema

Son aquellas personas autorizadas para acceder al sistema de información utilizando las posibilidades que les ofrece el mismo.

Los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del sistema, por lo tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio sistema.

2.9.6 La distribución en niveles de las responsabilidades

A menudo pueden distinguirse 3 niveles en el organigrama de una organización:



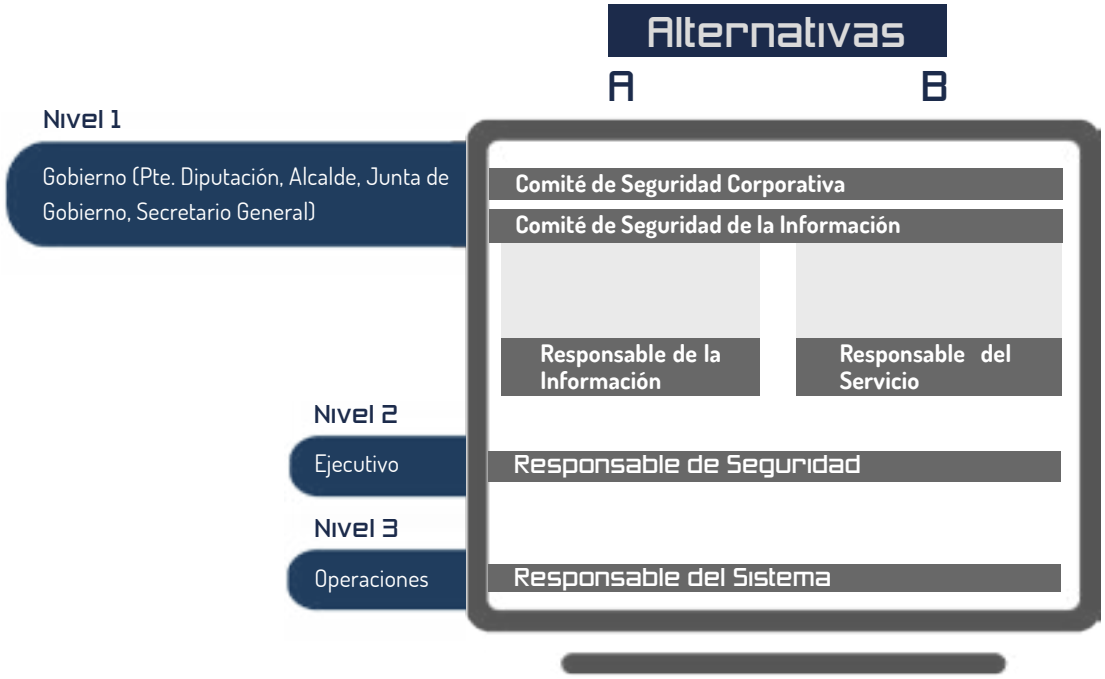
Como hemos dicho:

- El Responsable de la Información estará en el Nivel 1.
- El Responsable de la Seguridad estará en el Nivel 2.
- El Responsable del Sistema estará en el Nivel 3.
- El Responsable del Servicio, cuando sea diferente del Responsable de la Información, estará en el Nivel 1 o en el Nivel 2, dependiendo del organigrama de la organización.

> Cuando exista un Comité de Seguridad Corporativa, estará en el Nivel 1.

> Cuando exista un Comité de Seguridad de la Información, estará en el Nivel 1.

El cuadro siguiente esquematiza esta disposición.



LOS USUARIOS JUEGAN UN PAPEL FUNDAMENTAL EN EL MANTENIMIENTO DE LA SEGURIDAD DEL SISTEMA, POR LO TANTO, ES PRIMORDIAL SU CONCIENCIACIÓN EN LA SEGURIDAD DE LAS TIC

2.9.7 El Comité de Seguridad de la Información

Si el tamaño de la entidad local lo permite, suele ser frecuente que, por encima de todos los actores citados, exista un **Comité de Seguridad de la Información** que aúne las responsabilidades sobre información y servicios.

Este Comité se articulará y funcionará como un órgano colegiado de acuerdo con la normativa administrativa, facilitando la armonía de las diferentes partes de la organización y coordinando la seguridad de la información a nivel de organización.

La seguridad de la información necesita estar coordinada, tanto en los Ayuntamientos como en las funciones transversales de las Diputaciones Provinciales, para **racionalizar el gasto** y para **evitar disfunciones** que posibiliten la existencia de brechas de seguridad no controladas.

Son funciones típicas del Comité de Seguridad de la Información:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos (Concejalías, etc.)
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Alta Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico o jurídico, propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Asesoría externa
- Grupos de trabajo especializados internos, externos o mixtos.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias

LA SEGURIDAD DE LA INFORMACIÓN NECESITA ESTAR COORDINADA, TANTO EN LOS AYUNTAMIENTOS COMO EN LAS FUNCIONES TRANSVERSALES DE LAS DIPUTACIONES PROVINCIALES

Es conveniente que el Responsable de la Seguridad de la Información del sistema (Responsable de la Seguridad en el ENS) sea el secretario del Comité de Seguridad de la Información y como tal:

- Convocará las reuniones del Comité de Seguridad de la Información
- Preparará los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones
- Elaborará el acta de las reuniones
- Será responsable de la ejecución directa o delegada de las decisiones del Comité

2.9.8 Nombramientos

La Dirección de la entidad (Presidente Diputación, Alcalde, Junta de Gobierno) nombrará:

- Al Responsable de la Información (que puede tratarse de una persona o un órgano colegiado -típicamente, el Comité de Seguridad de la Información-) y al Responsable del Servicio (que puede ser el mismo que el anterior).
- El Responsable de la Seguridad, que debe reportar directamente a la Dirección o, cuando existan, a los comités de seguridad de la información y seguridad corporativa o al Responsable del Sistema, que, en materia de seguridad, debe reportar al Responsable de la Seguridad.

El procedimiento de nombramiento formal de los responsables mencionados debe constar en la Política de Seguridad de la Información de la entidad local.

2.9.9 Asignación de tareas y determinación de responsabilidades

Ver Anexo tareas y responsabilidades.

2.9.10 Competencias de las Diputaciones Provinciales

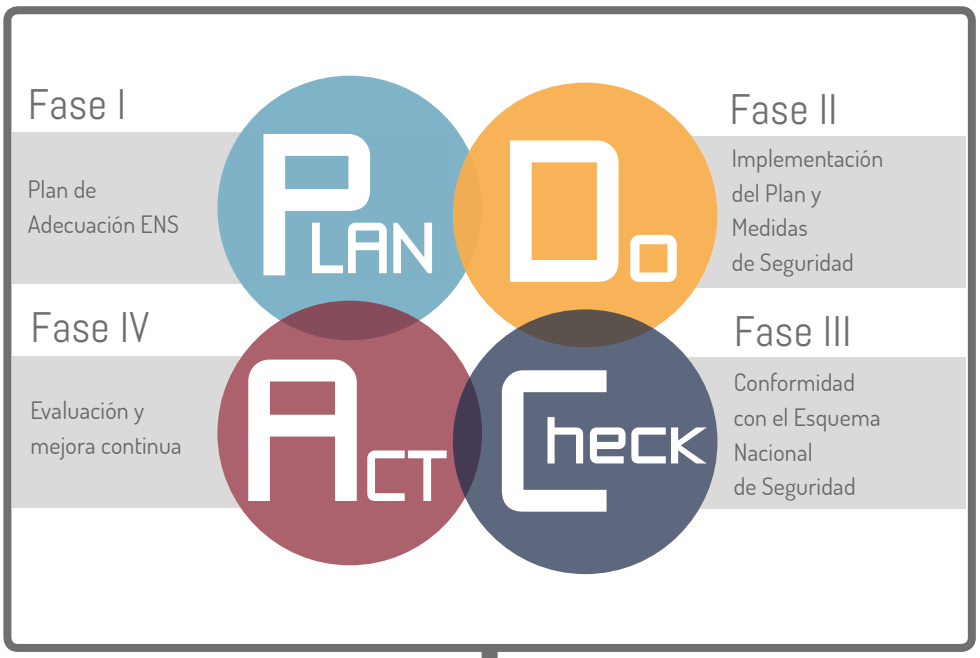
Hay que señalar que la nueva definición de competencias provinciales establecidas en la Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local, introduce una innovación esencial en relación con la implantación de la Administración Electrónica en los municipios, al atribuir a las diputaciones provinciales, en la nueva redacción dada al artículo 36 de la Ley reguladora de las Bases de Régimen Local, la **competencia para la prestación de los servicios de Administración Electrónica en los municipios con población inferior a 20.000 habitantes, entre ellos el soporte a la implantación del ENS**.

3

Diagrama General por fases

3.1 [FASES] Definición de las Fases Principales

Una de las principales variables determinantes en los proyectos de **implantación** del ENS se basa en la comprensión de los fundamentos básicos del modelo. A continuación, se detalla de forma simplificada, las principales fases de las que consta un proyecto de adecuación al ENS, bajo un enfoque práctico.



Herramientas CCN-CERT

Guías CCN-STIC

La analogía del proceso…

Comenzaremos este proceso descriptivo realizando una analogía con el concepto de **"implantar una prótesis"**, utilizado en el sector médico. Este concepto se define como *"la colocación de un elemento ajeno en el cuerpo de un ser vivo, mediante una intervención quirúrgica, para mejorar su funcionamiento"*.

Tras la intervención, existe un riesgo de fracaso, inducido por las propias células del cuerpo, que se resisten al elemento extraño atacándolo. Este símil representa uno de los retos para alcanzar el éxito, la resistencia al cambio por parte de las personas de la organización.

Este tipo de proyectos requieren aplicar el conocido del principio de proporcionalidad, buscando un equilibrio razonable que permita hacer factible la implantación de las medidas de seguridad en el Ayuntamiento. Por ejemplo, en el caso de los Ayuntamientos de menor población, es muy común la falta de recursos, tanto económicos como de personal. Por ello, se deberá establecer un proceso de implantación gradual, basado en hitos de madurez y, recorriendo las diferentes fases con el apoyo de las Diputaciones.

3.1.1 [FASE 01] Desarrollo de un Plan de Adecuación ENS

Objetivo

La elaboración del denominado Plan de Adecuación, es el punto de partida para adecuar nuestro Ayuntamiento al ENS. Nos permitirá organizarnos, mediante la asignación de **responsabilidades**, y planificar la implantación de las medidas de seguridad que necesitamos para poder cumplir con la normativa, que serán identificadas a través de un proceso de auditoría, similar a otros procesos de cumplimiento normativo.

Las insuficiencias detectadas se traducirán en la ejecución de las tareas priorizadas a través de hoja de ruta (Plan de Mejora), identificando para cada una de las insuficiencias, el responsable de ejecución, de supervisión, su plazo previsto, así como una estimación de su coste, cuantificado o bien en horas de personal o bien partidas presupuestarias para la adquisición de bienes y/o servicios.

Descripción general. Fase 1-Elaboración del Plan de Adecuación

1 PLANIFICACIÓN

Asignación de responsabilidades
Fijación del Contenido del Plan

CCN-STIC-806 Plan de Adecuación al ENS

2 POLÍTICA DE SEGURIDAD

Preparación y aprobación de la Política de Seguridad
Definición de roles y asignación de personas
Modelo de organización de la seguridad

CCN-STIC-805 Política de Seguridad de la Información
CCN-STIC-801 Responsabilidades y Funciones

3 DETERMINACIÓN DE LA CATEGORÍA DEL SISTEMA

Inventario de la Información y los Servicios (implicaciones de protección de datos)
Valorar la información y los servicios de cada una de sus dimensiones (disponibilidad, autenticidad, confidencialidad, integridad y trazabilidad) según "niveles de importancia": Bajo, Medio y Alto.
Valoración de la categoría de los sistemas: Básica, Media y Alta

CCN-STIC-803 Valoración de los sistemas
CCN-STIC-830 Ámbito de aplicación del ENS

4 Análisis de Riesgos

Identificación de activos (incluidas personas)
Valoración de amenazas y salvaguardas
Analizar impacto y riesgo
Herramienta de referencia: PILAR (metodología MAGERIT)

CCN-STIC-470H Manual de la Herramienta de Análisis de Riesgos PILAR

5 Declaración de aplicabilidad (SoA)

Documento con las medidas de seguridad que son de aplicación al sistema
Adecuación de los controles

CCN-STIC-804 Guía de Implantación del ENS

6 Informe de insuficiencias (Gap Analysis)

Informe de insuficiencias del sistema.
Estado ideal vs situación actual

7 Plan de Mejora

Hoja de ruta: tareas, plazos y recursos

¿Qué elementos componen nuestro plan de adecuación?

Un Plan de Adecuación debe estar compuesto, al menos, por los siguientes elementos:

- Política de Seguridad de la Información.
- Valoración de la Información y los Servicios a proteger. Correspondencia con el modelo actual de protección de datos.
- Definición del nivel de seguridad que resulta de aplicación (Categoría del Sistema)
- Realización de una evaluación de Riesgos.
- Declaración de Aplicabilidad (SoA)
- Insuficiencias del Sistema (Gap Analysis) con la asunción de riesgos.
- Plan de Mejora de la Seguridad o tratamiento de riesgos (actuaciones destinadas a subsanar insuficiencias detectadas.)

Guía de referencia general

» En la Guía CCN-STIC-806 Plan de Adecuación al ENS, desarrollada por el Centro Criptológico Nacional, encontrarás los principales detalles para la elaboración de un plan de adecuación.

Principales Tareas

La elaboración del Plan de Adecuación, consiste en la consecución ordenada de una serie de serie de pasos:

PASO 1: ELABORACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Este documento refleja el **compromiso** de la Administración en materia de seguridad. Por tanto, se trata de un documento de alto nivel que define lo que significa "seguridad de la información" en un Ayuntamiento. Deberá ser aprobado por el Órgano Superior (en las Diputaciones por la Presidencia y en los Ayuntamientos por la Alcaldía) promoviendo su difusión mediante su publicación en el correspondiente Boletín Oficial de la Provincia.

> Para su elaboración nos servirá de base la guía CCN-STIC-805 Política de Seguridad de la Información que aparte, de explicar la finalidad de esta política nos propone un modelo a seguir.

Esta Política de Seguridad es un documento estratégico. Una vez aprobada y publicada, su principal objetivo es que se **adquieren compromisos públicos**. Como por ejemplo, el establecimiento de planes anuales de concienciación para todo el personal (buen uso de los sistemas, riesgos en el uso de redes públicas,...), formación específica asociada al puesto de trabajo a desempeñar, la actualización del análisis de riesgos con periodicidad al menos anual, etc.

Uno de los aspectos más importantes que se contemplan en la política de seguridad es la creación de un modelo para la organización de la seguridad, es decir, la atribución de un modelo basado en funciones y responsabilidades (Comité de Seguridad y Roles) con una búsqueda de implicación en la organización.

> La guía CCN-STIC-801 Responsabilidades y funciones del ENS proporciona información sobre las responsabilidades de los diferentes de roles de seguridad, las dependencias funcionales, la delegación de funciones, etc.

Para la elección de estos roles deberemos tener en cuenta el artículo 10 del Real Decreto 3/2010 relativo al concepto de " La seguridad como función diferenciada ": el Responsable de Seguridad deberá ser independiente del Responsable del Sistema. Aspecto bastante complicado en pequeños ayuntamientos. Una posible solución reside en las Diputaciones, pudiendo desempeñar parte del proceso de diferenciación, asumiendo la responsabilidad del sistema, de forma que mejor se cumpla esta función diferenciada.

En cuanto a la composición del Comité, en los anexos de la guía se establecen ejemplos para diferentes estructuras, en función de las dimensiones de la Administración. **En la práctica y como norma general**, los comités de seguridad deben de disponer un enfoque muy ejecutivo, lo que normalmente se traduce en estructuras muy reducidas de personas y presididas por un cargo político (p.ej. Alcalde/sa)

PASO 2: IDENTIFICACIÓN DE LA INFORMACIÓN Y LOS SERVICIOS. DETERMINACIÓN DE LA CATEGORÍA DEL SISTEMA

El siguiente paso será **identificar la información y los servicios prestados**, objeto de protección. Determinar el "nivel de importancia" que tienen para nuestro Ayuntamiento. Se valora el nivel crítico de diferentes características, a las que denominaremos dimensiones, pudiendo asignar diferentes valores a cada una de sus dimensiones.

El **inventario de la Información y los Servicios** deberá estar relacionado con el actual modelo de protección de datos. Eso supone que deberá establecer la relación con el inventario de tratamientos que establecerá el Reglamento General de Protección de Datos, o en su defecto mientras resulte de aplicación, con los ficheros de la normativa LOPD.

Con la entrada en vigor de 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, el marco de aplicación material **deberá de extenderse a todos los elementos y en particular aquellos que contribuyen a desarrollar el procedimiento administrativo**.

A continuación se detallan algunos ejemplos de sistemas que están dentro del ámbito de aplicación material: tramitación de expedientes, el padrón municipal de habitantes, el perfil de contratante, portal de transparencia, la gestión contable, gestión tributaria, portal del empleado, video vigilancia en espacios públicos, etc.

Determinados los sistemas se identificarán los servicios e información soportados por cada uno de ellos, identificando aquella información que esté sujeta a la normativa vigente en materia de protección de datos de carácter personal.

SERVICIOS PRESTADOS	INFORMACIÓN NECESARIA	SISTEMA DE INFORMACIÓN	IMPLICACIONES LOPD
Servicios vinculados al Padrón Municipal de Habitantes (Altas, certificados, bajas, etc.)	Padrón Municipal de Habitantes	Gestión de padrón	Fichero relativo al Padrón Municipal de Habitantes
Gestión de subvenciones	> Expedientes administrativos > Gestión de subvenciones > Gestión económica	Gestión de expedientes	Fichero/s vinculados a la gestión de subvenciones
Seguridad Ciudadana	> Actuaciones Policiales > Sistemas video vigilancia	> Gestión Policial > Videovigilancia	> Gestión Policial > Video vigilancia

No todos estos sistemas requieren las mismas medidas de seguridad. Para determinar la categoría de los sistemas, se deberá proceder a valorar la información y los servicios en cada una de sus dimensiones de seguridad (Disponibilidad [D], Autenticidad [A], Confidencialidad [C], Integridad [I], Trazabilidad [T]). Se trata de establecer "niveles de importancia" sobre cada una de las dimensiones.

Pero en realidad, ¿qué significa cada una de estas dimensiones? Veamos algunos ejemplos:

- La **disponibilidad** actúa sobre la no interrupción del servicio (p.ej. La Web corporativa, perfil de contratante o algunos trámites electrónicos en la sede dejan de funcionar y no están accesible a través de internet.)
- La **autenticidad** protege el aseguramiento de la identidad (p.ej. La identidad de la persona que ha firmado un documento, quién se ha conectado a través de una red WIFI, etc.)
- La **confidencialidad** previene la filtración de información (p.ej. Gestionar el acceso a determinado tipo de información.)
- La **integridad** previene manipulaciones de la información (p.ej. Disponer de documentos que han sido firmados de forma electrónica, asegurar la fecha de publicación de un documento en la sede electrónica, etc.)
- La **trazabilidad** permite conocer posibles rastros en accesos (p.ej. sistema de registro de accesos por parte de usuario, análisis de posibles fugas de datos, intrusión a sistemas de ataques externos, etc.)

Valorar la información simplemente es atribuir "niveles de importancia" en cada dimensión. Los posibles valores se clasifican en Bajo, Medio y Alto. Es muy importante no confundir la valoración del ENS con la clasificación de los niveles tradicionales de la LOPD, ya que tienen diferentes criterios (Ver Instrucciones del anexo I del Real Decreto ENS) **Los ficheros de nivel ALTO en protección de datos no tienen por qué ser considerados como "nivel ALTO" en ENS.**

En protección de datos, el nivel de protección se determina en función de la tipología de los ficheros, aspecto que cambiará en el Reglamento General de Protección de Datos. En cambio, en ENS la categoría viene determinada por los niveles asociados a sus dimensiones que siguen otros criterios.

¿Qué categoría tiene mi Ayuntamiento? La regla general tiende a MEDIA

Veamos el siguiente ejemplo, analizamos la importancia de la disponibilidad de una plataforma web que permite la presentación de ofertas a los licitadores para contratos menores. El nivel de criticidad de la dimensión de disponibilidad de la plataforma (web no disponible) quizás tenga una mayor relevancia para el Ayuntamiento frente a otros sistemas como por ejemplo el portal de transparencia municipal, ya que la presentación de ofertas en procesos de licitación precisa tener accesible la plataforma durante un plazo establecido.

No obstante, si comparamos el nivel de criticidad de este servicio de licitación frente a otros, como por ejemplo, el control de tráfico aéreo de un aeropuerto, veremos que la plataforma de contratación es crítica pero no tanto como este último.

Es por ello, que debemos establecer criterios de valoración basados en la importancia relativa, para evitar disponer de sistemas de categoría ALTA de forma generalizada, ya que el nivel real de exigencia es muy alto y está pensado para sistemas críticos.

¿Quién valora la información y los servicios?

En la política de seguridad, que aprobamos en el primer paso, se definen los roles y responsabilidades:

- La información y los servicios (Bajo, Medio y Alto) deberían ser valorados, como norma general, por parte de los responsables de las áreas, utilizando criterios homogéneos de valoración, definidos con anterioridad.
- La Categoría del Sistema que soportan los servicios y la información (Básica, Media y Alta) y con ello la determinación de las medidas de seguridad mínimas que será necesario aplicar, deberá ser determinada por el Responsable del mismo, pudiéndose recabar propuesta del Responsable de Seguridad, teniendo en cuenta las valoraciones indicadas en el punto anterior, conforme a las instrucciones del anexo I del Real Decreto ENS.

Para realizar la valoración nos apoyaremos también en la Guía CCN-STIC-803 Valoración de los sistemas, que complementa los criterios establecidos en el anexo I del RD 3/2010. Para la identificación deberemos tener en cuenta el nuevo alcance definido por la entrada en vigor de la Ley 39/2015 y Ley 40/2015 plasmado en el ámbito objetivo definido en la Guía CCN-STIC-830 Ámbito de Aplicación del Esquema Nacional de Seguridad, todas y cada una de las actuaciones que contribuyan a desarrollar el procedimiento administrativo. Aunque lo conveniente es aplicar el ENS a todos los sistemas de información.

En aquellos casos, en los que no se haya podido designar algunos Responsables de Información y/o Servicios, o no se haya podido valorar formalmente, esta valoración podrá ser realizada, de manera provisional, por el Responsable de Seguridad. Esta situación es muy habitual en las primeras etapas de ejecución del ENS. Conforme se aumenten los niveles de madurez, esta valoración deberá ser asumida por cada uno de los responsables de las diferentes áreas y departamentos. En el caso de Ayuntamientos de pequeña dimensión estas responsabilidades pueden ser asumidas por el Comité de Seguridad.

Tanto para la valoración de la Información como de los Servicios, será necesario disponer de conocimientos legales y/o técnicos en la materia que se trate, por lo que habrá que tener en cuenta su naturaleza y la normativa de aplicación, aspectos que deberán ser considerados en la elaboración de los planes formativos.

En el Anexo se puede encontrar un ejemplo que ayudará a comprender cómo valorar un sistema como el del ejemplo formado por 2 servicios.

Servicios Prestados por otras Administraciones Públicas

En la actualidad, debido a la reducción de su capacidad económica y a una insuficiencia en su capacidad técnica, cada vez son más las entidades locales que recurren a servicios prestados por otras administraciones (Diputaciones, Comunidades Autónomas y Administración General del Estado). Es más, la disposición adicional segunda determina que "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.", lo que anima prácticamente al uso casi obligatorio de los servicios proporcionados por la Administración General del Estado.

A partir del 5 de noviembre de 2017 los sistemas de información de todas las Administraciones Públicas deberán adecuarse a lo dispuesto en la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015. En esta fecha podemos presumir la adecuación al ENS de los servicios prestados por todas las Administraciones Públicas, incluyendo los prestados a otras administraciones, aunque la realidad nos hace pensar que pueden darse casos en los que no esté materializada en su totalidad tal adecuación.

Por todo ello desde las Entidades Locales tenemos la obligación de exigir las Declaraciones o Certificaciones de Conformidad con el ENS, en el ámbito concreto de la prestación, independientemente de que sea un prestador público o privado, porque no deja de ser responsabilidad de la Entidad Local, a través de la figura del Responsable de Seguridad, el velar por la certificación de los servicios utilizados y asegurarse de que su uso no suponga una amenaza o riesgo en la seguridad integral de la organización.

La valoración de los servicios prestados por terceros (empresas privadas)

Una de las principales novedades del ENS recae sobre los prestadores de servicios. Las soluciones y servicios prestados por el sector privado (proveedores tecnológicos), comprendidos dentro del ámbito objetivo, **deberán de satisfacer las exigencias legales establecidas en el mismo**. Es por ello, que **se deberán requerir/exigir en los procesos de licitación garantías de cumplimiento**. En este sentido deberemos identificar el nivel mínimo exigible de certificación, y lo que es más importante, definir el alcance concreto, para asegurarnos de que la certificación del prestador cubre el objeto del servicio. A continuación se detallan algunos ejemplos concretos.

A PARTIR DEL 5 DE NOVIEMBRE DE 2017 LOS SISTEMAS DE INFORMACIÓN DE TODAS LAS ADMINISTRACIONES PÚBLICAS DEBERÁN ADECUARSE A LO DISPUESTO EN LA MODIFICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

EJEMPLO	DESCRIPCIÓN	¿Requiere pedir Declaración/ Certificación ENS al proveedor?	Ver cláusula tipo para pliegos
Correo Electrónico	Soluciones de correo electrónico basadas en servicios Cloud.	**Podría precisar declaración / certificación** Sería preciso siempre que intervenga de forma esencial en el ejercicio de las competencias de las entidades locales y en el desarrollo del procedimiento administrativo.	Anexo Cláusulas 01
Herramientas colaborativas o de intercambio de información	Herramientas basadas en servicios de almacenamiento de archivos (Por ejemplo, un servicio de intercambio de ficheros en la nube)	**Requiere solicitar declaración / certificación.** Deberá cubrir la prestación y alojamiento de la información. El nivel mínimo exigible dependerá del tipo de información manejada, y de su importancia en el desenvolvimiento del procedimiento administrativo, que podría tener mayores implicaciones en el caso de tratar datos personales.	Anexo Cláusulas 02
Desarrollo de portales y sedes electrónicas	Desarrollo web de páginas web (por ejemplo, la propia sede electrónica, portal de transparencia, etc.)	**Requiere solicitar declaración / certificación** El alcance de la certificación deberá ser doble. Por un lado el desarrollo seguro del producto y por otro lado se deberá de cubrir la ubicación de la solución, en la modalidad que sea provisionada.	Anexo Cláusulas 03
Desarrollo de software	Empresas que desarrollan programas para la Administración (por ejemplo, gestor de expedientes, portal del empleado, gestión tributaria, desarrollo de una aplicación móvil de gestión de incidencias)	**Requiere solicitar declaración / certificación** El alcance de la certificación deberá cubrir el desarrollo seguro del producto, para que introduzcan las medidas de seguridad necesarias para garantizar el cumplimiento del ENS en las entidades locales, así como posibles tareas de instalación y soporte.	Anexo Cláusulas 04
Control de acceso	Sistemas de control de identificación y/o sistema de venta de entradas (en este caso podrían aplicar otros estándares como PCI DSS)	**Requiere solicitar declaración/ certificación** El alcance de la certificación debe de contemplar al menos el propio desarrollo del producto.	Anexo Cláusulas 05

EJEMPLO	DESCRIPCIÓN	¿Requiere pedir Declaración/ Certificación ENS al proveedor?	Ver cláusula tipo para pliegos
Sistemas de Ciudades Inteligentes e Internet de las Cosas	Soluciones vinculadas con el desarrollo de productos, servicios o plataformas Smart, incluyendo Sistemas SCADA *(Supervisory Control and Data Acquisition)*, como por ejemplo sistemas de control semafórico, alumbrado inteligente, etc.	**Requiere solicitar declaración / certificación** El alcance deberá cubrir la prestación completa de la solución y/o servicio. Este tipo de sistemas son especialmente críticos, ya que existe una falta de madurez, en materia de seguridad, en los sistemas industriales.	Anexo Cláusulas 06
Empresas de consultoría	Empresas que desarrollan procesos de consultoría, como por ejemplo el desarrollo de un plan estratégico de ciudad, estudios de impacto, etc.	**NO precisa declaración ni certificación**	N/A
Empresas de consultoría y servicios de seguridad	Empresas proveen de soluciones, como por ejemplo soluciones de monitorización de equipos	**Requiere solicitar declaración / certificación** Requiere certificación que cubra la forma en la que se desarrolla la prestación del servicio. En caso de la existencia de productos de seguridad se deberá analizar la utilización adicional de productos certificados.	Anexo Cláusulas 07
Servicios de implantación de administración electrónica en la propia Entidad *(on premise).*	Fabricante de solución que instala su aplicación en las dependencias municipales	**Requiere solicitar declaración / certificación** El alcance deberá de cubrir el desarrollo seguro de software, para que introduzcan las medidas de seguridad necesarias para garantizar el cumplimiento del ENS en las entidades locales, así como los servicios de implantación y soporte.	Anexo Cláusulas 08
Servicios de formación	Empresas que prestan servicios de formación presencial	**NO precisa certificación**	N/A

Servicios Cloud para implantación de administración electrónica	Empresas que prestan servicios en sistemas basados en la nube	**Requiere solicitar declaración/ certificación** El alcance deberá de cubrir el desarrollo de software de la solución, los servicios de implantación y soporte, así como la ubicación de la información (que puede ser en un segundo proveedor)	Anexo Cláusulas 09
Empresas de limpieza	Empresas que prestan servicios de limpieza en las dependencias municipales	**NO precisa declaración ni certificación**	N/A
Sistemas de videovigilancia	Cámaras instaladas en los Ayuntamientos (seguridad ciudadana, tráfico, acceso a edificios)	**No precisa declaración / certificación,** sin perjuicio de estar a lo que disponga la regulación sobre Protección de Datos.	Anexo Cláusulas 10
Servicios municipales	Servicios como la zona AZUL, préstamo de bicicletas, etc., en las que se utiliza algún tipo de sistema, como por ejemplo una APP móvil	**Requiere solicitar declaración / certificación** El alcance deberá de cubrir al menos el desarrollo seguro de la solución software que se aporta.	Anexo Cláusulas 11

Con carácter general se pueden diferenciar tres tipos:

1. Pedir la certificación a las **empresas que desarrollan software** de forma que cubra el ciclo de desarrollo seguro. Si el ámbito es el desarrollo de software, el producto resultante debe de ser seguro y debería cubrir las funcionalidades de seguridad establecidas en la Ley 39 y 40 así como las vinculadas al GDPR y ENS propiamente dichas Ej. (Implantación de portales para Ayuntamientos, páginas web de turismo, que muchas veces se crean a través de pequeñas empresas que montan un WordPress /Drupal y no hay consideraciones en el despliegue en materia de seguridad).
2. Pedir la certificación a **empresas que prestan servicios** de soporte de sistemas, procesos de implantación o soporte. Por ejemplo, cuando un proveedor se conecta en remoto o recibe una base de datos porque no funciona la contabilidad, migraciones... En este caso, tenemos que regular bien los protocolos de acceso e intercambio. Podemos encontrarnos desde la externalización global de un Ayuntamiento, implantaciones tradicionales en la propia Entidad, hasta pequeñas asistencias técnicas donde las empresas llevan el mantenimiento de la microinformática/impresoras o algunos elementos de red o pequeños servidores, como es la implantación de un gestor de expedientes).
3. Y el más importante, **Servicios Cloud puros prestados desde un tercero**. Lo habitual es la subcontratación, es decir, una empresa tiene un software y a su vez usa un Datacenter de un tercero, como podría ser el caso de una empresa prestadora de un servicio que se apoya a su vez en el CPD de un tercero).

PASO 3: EL ANÁLISIS DE RIESGOS

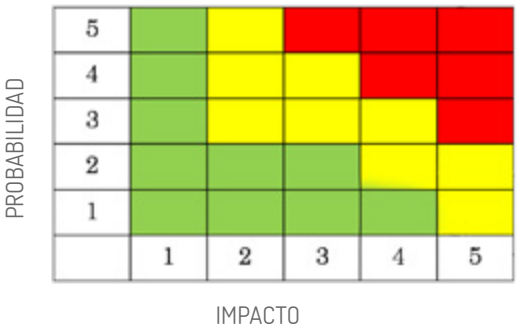
El siguiente paso consiste en analizar la confianza de los sistemas de información con los que trabajamos, pues cada vez es mayor nuestro grado de dependencia. La confianza depende no sólo de los fallos del propio sistema, sino de posibles errores humanos del personal interno, fallos de proveedores, catástrofes naturales, posibles ataques de seguridad de terceros, etc. Es por ello que los sistemas no sólo deben prevenir, sino reaccionar frente a incidentes que se puedan materializar.

En este punto, lo recomendable es hacer simulaciones frente a posibles incidentes de seguridad, que en cierto modo, consistirían en hacernos preguntas tales como:

- ¿Qué consecuencias podría tener en mi Ayuntamiento la pérdida de información motivada por la entrada de un virus que cifra la información?
- ¿Cómo podría afectar un desastre natural sobre la información municipal? Por ejemplo ¿y si se produce un incendio en la casa consistorial?
- ¿Cómo afecta que alguien suplante la identidad, en una red social, de un concejal del Ayuntamiento?
- ¿Qué efectos puede producir que se manipule el sistema de control de tráfico de la ciudad? ¿Y la página web del Ayuntamiento?

Este proceso de análisis de situaciones, es lo que se conoce como **análisis de riesgos**. **Para que los sistemas funcionen deberemos conocer el mapa de dependencias** con los equipos y comunicaciones. **Es lo que se denominan activos, entre los cuales debemos identificar incluso a las propias personas**, ya que los errores humanos muchas veces son más frecuentes que los propios fallos del sistema.

Identificados los activos, el siguiente paso es **conocer las amenazas** a las que están expuestos. Serán diferentes para cada tipo de activo. No es lo mismo una amenaza de fuego –que afecta a activos físicos- que de un virus –con mayor **impacto** en la información-. En este sentido, se debe analizar tanto el potencial impacto (consecuencia que tiene en el Ayuntamiento) **como el riesgo** (la probabilidad de que ocurra el incidente). Con ello, el Ayuntamiento puede priorizar su estrategia en aquellos ámbitos de actuación con mayores consecuencias o donde la frecuencia es muy recurrente. En definitiva, se trata de tener una herramienta que permita medir variables clave y adoptar decisiones con criterio y rigor.



- Riesgos que necesitan **monitorización**: Planes de actuación detectivos
- Riesgos que necesitan **investigación**: Planes de actuación preventivos
- Riesgos que necesitan **mitigación**: Planes de actuación correctivos

La categoría del sistema, fijada con anterioridad, nos determinará el nivel de detalle que deberá tener el **análisis de riesgos**. En la categoría básica, será suficiente un análisis informal realizado en un lenguaje natural o semi-informal. En la categoría media se usará un lenguaje específico y en la alta, un lenguaje específico con fundamento matemático.

Para su realización, podemos utilizar cualquier herramienta que utilice una metodología contrastada y reconocida. Como Administración Pública tenemos a nuestra disposición la herramienta PILAR, que está desarrollada y financiada parcialmente por el CCN y utiliza la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que ha sido elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información y que está enfocada a las Administraciones Públicas. Este análisis determinará las medidas complementarias que será necesario aplicar.

Por último, el análisis de riesgos deberá ser revisando periódicamente, al menos anualmente, ya que el riesgo no sólo depende de los cambios del sistema, sino de los del entorno, como pueden ser la frecuencia de ataques externos o incluso cambios reguladores como las nuevas Leyes 39 y 40 de 2015 o el Reglamento Europeo de Protección de Datos.

En definitiva, necesitamos identificar activos esenciales, conocer qué amenazas existen, los efectos que producirían si se materializan y qué medidas de seguridad deben ser aplicadas, o bien reforzadas, para conseguir un nivel de riesgo aceptable para el Ayuntamiento.

PASO 4: LA DECLARACIÓN DE APLICABILIDAD (SoA[9])

En este punto, estaremos en condiciones de realizar la **Declaración de Aplicabilidad**, que consiste en la elaboración de un documento que recoge 1) las medidas de seguridad que son de aplicación a nuestro/s Sistema/s (Categoría Básica, Media o Alta); 2) otras medidas resultantes de la realización del análisis de riesgos y 3) aquellas otras que pudieran ser de aplicación a la Administración, como por ejemplo las establecidas por la normativa de protección de datos, sistemas de pago en cajeros (PCI DSS[10]), etc.

En esta declaración se motivará de manera precisa la adecuación de los controles, su exclusión o ampliación. **Es importante destacar que el modelo no es rígido, ya que tenemos la posibilidad de elegir alternativas de seguridad, siempre y cuando se justifique documentalmente** que protegen igual o mejor el riesgo sobre los activos afectados.

PASO 5: EL INFORME DE INSUFICIENCIAS *(GAP ANALYSIS)*

Las desviaciones al cumplimiento de las medidas de seguridad deberán recogerse en un documento, denominado informe de insuficiencias del sistema. Este informe, simplemente recoge la situación de cumplimiento de las medidas de seguridad (estado ideal vs situación actual.) Este informe deberá de ser aprobado por los **Responsables de la Información y de los Servicios**.

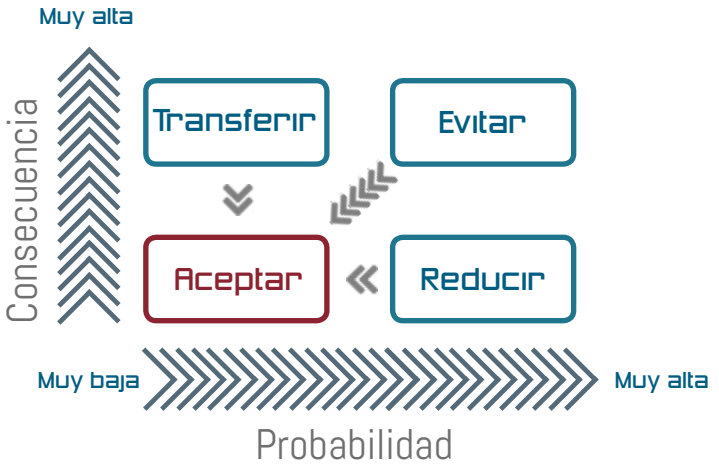
No existe la seguridad absoluta de nuestros sistemas, es por ello que los riesgos deben ser gestionados de forma objetiva. En algunos casos podrán ser incluso asumidos, lo denominaremos, riesgos residuales.

PASO 6: EL PLAN DE MEJORA DE LA SEGURIDAD (PLAN DE TRATAMIENTO DEL RIESGO)

Para finalizar, se definirán las tareas necesarias para subsanar las insuficiencias detectadas, indicando plazos, recursos asignados para su ejecución y se plasmarán en un documento denominado **Plan de Mejora de la Seguridad**.

[9] *Statement of Applicability*

[10] *Payment Card Industry Data Security Standard:* Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago



En los Ayuntamientos de menor población es interesante transferir el riesgo utilizando sistemas de terceros como, por ejemplo las Diputaciones. De esta forma, gran parte de las medidas de seguridad (NO TODAS) estarán cubiertas por el tercero de confianza, siempre y cuando esté certificado conforme ENS, garantice la categoría necesaria y el ámbito de la certificación este cubierto en la prestación del servicio.

Es conveniente que el Plan de Mejora, **sea aprobado formalmente** por la Administración, primeramente por el Comité de Seguridad de la Información, y posteriormente por parte del Alcalde / Presidente de la Administración Local, según sea el caso. De este modo conseguimos un compromiso formal por parte de la Administración.

MEDIDAS PRIORITARIAS	CONTROL	PLAZO EJECUCIÓN	RESPONSABLE EJECUCIÓN Y SUPERVISIÓN	COSTE
Designación de roles y asignación de Responsabilidades ENS y RGPD	org.1	Trimestre 1	...	€ /horas
Constitución del Comité de Seguridad de la Información	org.1	Trimestre 1	...	€ /horas
Aprobación y publicidad de la Política de Seguridad de la Información	org.1	Trimestre 2	...	€ /horas
Revisión y aprobación de la Política de Utilización de los Recursos y Sistemas de información. Difusión (publicación en la intranet y acciones formativas)	org.2	Trimestre 2	...	€ /horas
...			...	

MEDIDAS PRIORITARIAS	CONTROL	PLAZO EJECUCIÓN	RESPONSABLE EJECUCIÓN Y SUPERVISIÓN	COSTE
Auditoría de seguridad y pruebas de penetración (test de intrusión y un análisis de vulnerabilidades) de los trámites online, (tercero que acredite un informe positivo de dichas pruebas).	mp.sw.2	Trimestre 3	...	€ /horas
Implantación de un sistema de detección de intrusiones (IDS)	op.mon1.1	Trimestre 4	...	€ /horas

3.1.2 [FASE 02] Implementación del Plan de Adecuación

Objetivo

Llevar a cabo los compromisos adquiridos en el Plan de Mejora de la Seguridad. Implantación del ENS.

1 Revisión Plan de Adecuación

Realizar acciones del Plan
Supervisar los tiempos establecidos
Documentación para un Sistema de Gestión de Seguridad de la Información (SGSI)

2 Medidas de Seguridad: Marco Organizativo

Políticas de Seguridad
Normativa de Seguridad
Procedimientos de Seguridad
Proceso de Autorización

CCN-STIC-821 Normas de Seguridad en el ENS (y Anexos)
CCN-STIC-822 Procedimientos de Seguridad (y Anexos)

3 Medidas de Seguridad: Marco Operacional

Medidas de planificación
Control de acceso
Explotación
Servicios externos
Continuidad del servicio
Monitorización del sistema

CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS

4 Medidas de Protección

Protección de instalaciones, equipos y comunicaciones
Gestión del personal
Protección de los soportes y aplicaciones informáticas
Protección de información y servicios

CCN-STIC-807 Criptología de empleo en el ENS
CCN-STIC-811 Interconexión en el ENS
CCN-STIC-812 Seguridad en servicios web
CCN-STIC-814 Seguridad en servicio de correo
CCN-STIC-820 Protección contra Denegación de Servicio
CCN-STIC-835 Borrado de metadatos en el marco del ENS

ens Esquema Nacional de Seguridad

Descripción general

Construir un sistema organizado de gestión de la seguridad de la información, basado en políticas, procedimientos, instrucciones, registros, controles, activos, comportamientos, cultura, etc.

Guía de referencia general

El CCN proporciona las Guías CCN-STIC de Seguridad, que consisten en una serie de normas, instrucciones, guías y recomendaciones, dirigidas al personal de las Administraciones Públicas, proporcionadas a través de la parte privada de su portal web. También dispone de otras de difusión pública, es decir, accesibles a cualquier usuario; en concreto la serie 800 que versa sobre el ENS.

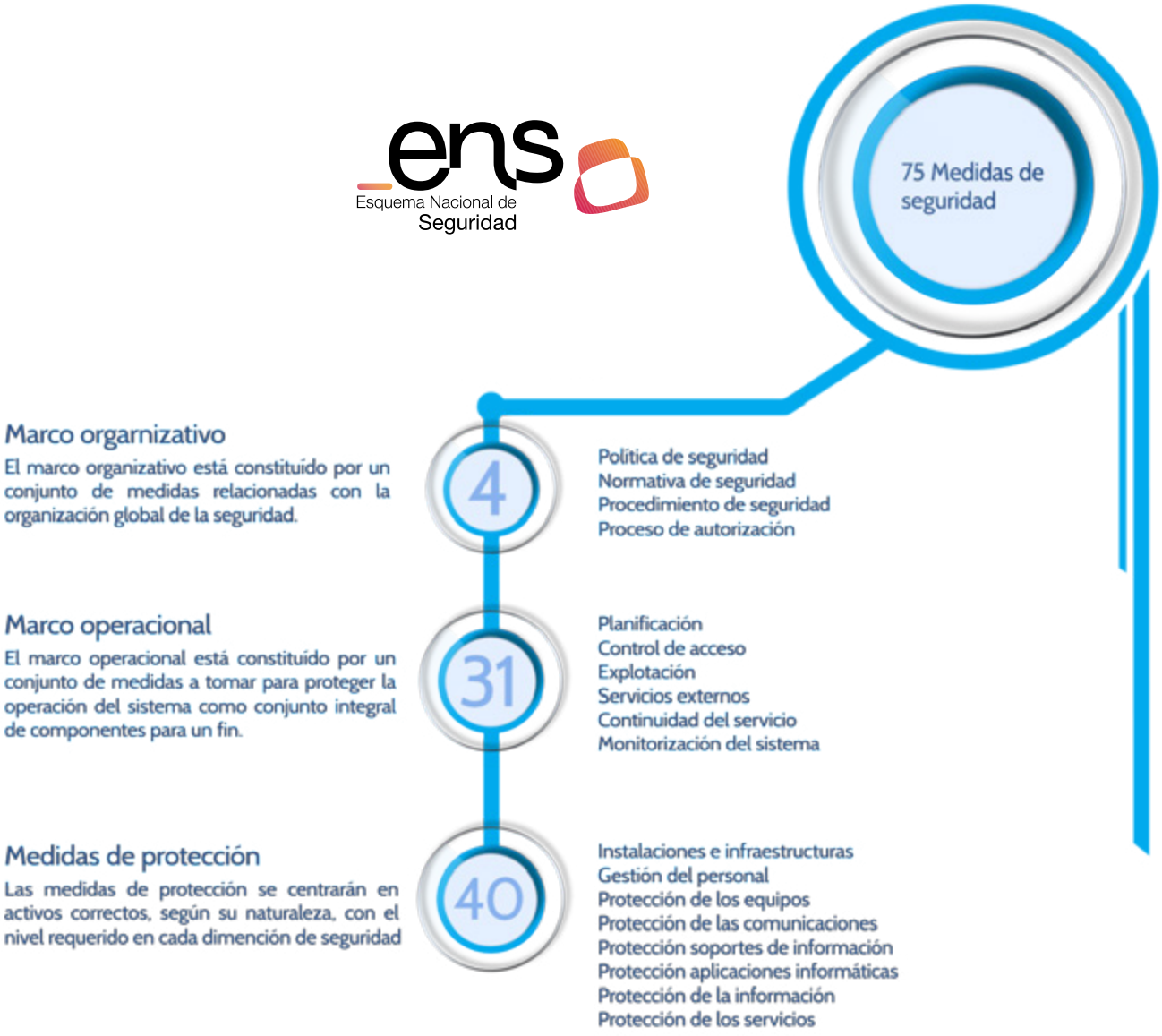
Este organismo, y en concreto su Capacidad de Respuesta a Incidentes, CCN-CERT, también pone a nuestra disposición una serie de herramientas que nos servirán de ayuda para garantizar y gestionar la seguridad de la información:

INTERACCIÓN ENTRE HERRAMIENTAS

1. Sistema de Alerta Temprana en Internet
2. Sistema de Alerta Temprana en la red Sara
3. Detección de APT
4. Análisis dinámico de ficheros
5. Multiantivirus
6. Análisis y gestión de riesgos
7. Auditoría de cumplimiento ENS/STIC
8. Informe de estado de seguridad en el ENS
9. Inspección de dispositivos de red
10. Entornos clasificados
11. Gestión de ciberincidentes
12. Investigación de ciberincidentes y compartición de inform
13. Almacenamiento en la nube
14. Plataforma de retransmisión (streaming)

Principales Tareas

Para llevar a cabo la implementación del ENS, se llevaran a cabo las acciones recogidas en el Plan de Mejora de la Seguridad, supervisando la ejecución de las tareas en los tiempos establecidos. Igualmente, se irá desarrollando el fondo documental que dará soporte a la gestión de la seguridad de la información. Inicialmente, parece lógico llevar a cabo el proceso de implantación siguiendo el orden que presentan las medidas de seguridad recogidas en el anexo II del Real Decreto ENS, cimentando las normas implantando las medidas del "marco organizativo", para seguir con las medidas de seguridad que garantizan las operaciones sobre el sistema para continuar con las medidas de protección de los activos. A continuación se analizan cada grupo brevemente:



Visión simplificada de las medidas de seguridad

Con el objetivo de simplificar la guía se realizará un resumen de las principales medidas de seguridad. En los Ayuntamientos de menor población la clave de cumplimiento reside en apoyarse en las Diputaciones o proveedores de confianza, para concentrar la mayoría de las medidas de seguridad de carácter tecnológico, sin que ello implica una pérdida de control efectivo.

Marco Organizativo

Definición de una normativa de seguridad: Se deberá regular el uso de los medios tecnológicos que pone a disposición el Ayuntamiento al personal para el desarrollo de sus funciones. Básicamente, consiste en una serie de documentos que regulan el uso correcto de equipos, servicios e instalaciones, detallando lo que se considera uso indebido, y la responsabilidad del incumplimiento o violación de estas normas.

Para su desarrollo nos servirán de base la Guía CCN-STIC-821 Normas de Seguridad en el ENS y sus Anexos. A su vez, la guía contiene subguías que regulan los siguientes elementos:

- Normativa general de utilización de los recursos y sistemas de información del organismo.
- Normas específicas o particulares. Normas de acceso a internet.
- Normas de uso de correo electrónico (e-mail)
- Normas para trabajar fuera de las instalaciones del organismo.
- Normas de creación y uso de contraseñas.
- Acuerdo de confidencialidad a terceros.
- Modelo de contenido de buenas prácticas para terceros

La aprobación de la reglamentación deberá ser sometida a la previa audiencia de la Juntas de Personal y del Comité de Empresa (en los términos previstos en los artículos 40 del Estatuto Básico del Empleado Público y 64.5 f) del Estatuto de los Trabajadores) y serán comunicados de manera fehaciente a los empleados públicos. Si queremos abordar la implantación de esta medida con éxito, es conveniente planificar acciones formativas y/o de concienciación para instruir en su aplicación. Igualmente será necesario establecer acciones de control de lo descrito en la misma y llevar a cabo las consecuencias de su incumplimiento. A la hora de desarrollar esta norma, deberemos prestar especial interés a la regulación del uso de los dispositivos móviles, ya que recientes informes de amenazas del CCN-CERT confirman a estos dispositivos como uno de los objetivos principales de las Ciberamenazas para el año 2017. Ver informe CCN-CERT BP-03/16 Buenas Prácticas en Dispositivos Móviles.

BYOD ***(Bring Your Own Device)*** trata de políticas y medidas de seguridad para acceder a recursos de la Administración a través de dispositivos personales, como por ejemplo, tener instalado el correo electrónico en el móvil personal. Este tipo de situaciones implica la adopción de algunos riesgos en materia de seguridad. Existen soluciones tecnológicas especializadas en dar cobertura a este paradigma, como por ejemplo MDM ***(Mobile Device Management)*** que permiten separar entornos personales y profesionales para administrar de forma segura los dispositivos.

El siguiente paso será el desarrollo de **Procedimientos de Seguridad**. Es de vital importancia que las principales tareas sobre el sistema de información se encuentren documentadas, con una asignación precisa de responsabilidades. **El principal objetivo de esta medida es evitar que el "conocimiento" solo resida en las cabezas de las personas (internas o externas)**, algo que por desgracia es muy habitual

> Para su desarrollo nos servirá de base la Guía CCN-STIC-822 Procedimientos de Seguridad y sus anexos.

Por último se deberá regular un **Proceso de Autorización** que nos permita gestionar de forma correcta la entrada de nuevos elementos en el sistema, como puede ser la entrada de equipos y/o aplicaciones en producción, la utilización de medios de comunicación, la utilización de soportes de información y de equipos móviles o la utilización de servicios de terceros bajo, contrato o convenio.

Marco Operacional

El siguiente grupo de medidas busca garantizar las operaciones del sistema mediante el establecimiento de medidas de seguridad que las protejan:

Medidas de planificación:

Encaminadas a planificar el sistema, consistentes en la gestión de los riesgos. Se trata fundamentalmente de:

- Realización e interpretación del ***Análisis de riesgos***.
- Documentación y la gestión de la ***Arquitectura de Seguridad***. En caso de Ayuntamientos de pequeña población cuya información resida en Diputación, ésta será la responsable de su documentación.
- Implantación de un proceso formal para la ***Adquisición de Nuevos Componentes y Dimensionamiento/ Gestión de capacidades***, evaluando las necesidades de procesamiento, almacenamiento de información, comunicación, personal, así como de instalaciones antes de la puesta en explotación. En el caso de Ayuntamientos de menor población cuya información resida en Diputación, será responsabilidad fundamentalmente de la misma.
- En caso de disponer de sistemas de categoría ALTA, los productos de seguridad que se adquieran (no las soluciones software de gestión) requerirán la denominada certificación de producto ***(Componentes Certificados)***. Por ejemplo, la utilización de un sistema de impresión que utilice un software de borrado seguro de los documentos que almacena en su cola de impresión.

Control de acceso:

Conjunto de medidas encaminadas a garantizar un correcto acceso a los recursos por parte de los usuarios o procesos acorde a las políticas de la Administración y que se encuentren previamente autorizados por los responsables correspondientes.

- Establecer mecanismos de identificación y autenticación. Esto implica tener identificado de forma unívoca todos los accesos al sistema, evitando utilizar cuentas comunes o compartiendo las contraseñas.
- Realización de una adecuada gestión de contraseñas (complejidad mínima, cambio periódico, etc.)
- Establecer roles para definir quién puede acceder a determinados recursos
- Regular el acceso remoto, utilizando equipos y conexiones de confianza.

Explotación:

Conjunto de medidas encaminadas a la protección de los activos. Para ello se precisa de:

- Hacer un ***Inventario de activos*** del sistema y la asignación de propietarios de los mismos. Se deberá disponer de un control de que servidores, equipos portátiles, teléfonos móviles, etc. que existen en el Ayuntamiento.
- Los equipos deben de estar correctamente configurados. Es lo que se denomina regular la ***Configuración de seguridad***, asegurando la configuración de los componentes del sistema manteniendo las reglas de "funcionalidad mínima", "seguridad por defecto". Por ejemplo, el personal no informático no puedan ser administradores locales de sus máquinas, los navegadores no deberán almacenar las contraseñas de los accesos, se deberán cambiar las contraseñas que vienen por defecto al adquirir componentes, etc.
- Proteger los activos frente a amenazas, como por ejemplo sistemas de antivirus, o protección frente a código dañino, etc.
- Gestionar los efectos que se produjeran sobre los mismos la materialización de estas amenazas "aprendiendo" de ellas. Para ello se precisa registrar las incidencias.
- Analizar la actividad de los usuarios sobre el sistema ***(Registro de la actividad de los usuarios)*** protegiendo estos registros de manipulaciones no autorizadas ***(Protección de los registros de actividad)***.
- Protección de las claves criptográficas (contraseñas) durante todo su ciclo de vida, generación, transporte, custodia, archivo y destrucción, como por ejemplo la utilización de aplicaciones adecuadas para almacenar las contraseñas.

Como norma general la clave es personal e intransferible, no debiendo ser conocida por nadie.

Servicios externos:

Antes de la utilización de recursos externos, servicios, equipos, instalaciones o personal, se deben establecer entre los requisitos contractuales. Se trata fundamentalmente de seguir el modelo "in eligiendo in vigilando".

- In Eligiendo: Previo al proceso de contratación se exigirán garantías de cumplimiento, solicitar certificación de conformidad ENS al prestador del servicio, acordando los denominados acuerdos de nivel de servicio (ANS)
- In Vigilando: Una vez se han contratado los servicios se deberán implementar mecanismos que permitan medir el cumplimiento de las obligaciones establecidas en los contratos. En el caso de que la disponibilidad [D] del sistema alcance el nivel alto, tendremos que garantizar la provisión del servicio por Medios Alternativos

Continuidad:

Conjunto de medidas conducentes a garantizar la continuidad de los servicios.

- Si la categoría de nuestro sistema es de nivel media, nos bastará con realizar un ***Análisis de Impacto*** (Business Impact Analysis o BIA), que identifica las necesidades en términos de recuperación, centrándose en aquellas que son indispensables. Analiza cómo impacta (daño reputacional, incumplimiento normativo, financiero...) así como un tiempo de recuperación objetivo (Recovery Time Objective o RTO). Así se identifican los elementos críticos para la prestación de cada servicio.
- Si la disponibilidad [D] de nuestro sistema alcanza un nivel alto, tendremos que desarrollar un proceso más formal, a través de un ***Plan de Continuidad***, que establezca las acciones a realizar en caso de interrupción de los servicios, así como ***Pruebas Periódicas***.

Monitorización:

Conjunto de medidas, conducentes a evaluar la eficacia del sistema mediante la medición de su actividad:

- Se precisa disponer de herramientas de detección o prevención de intrusión (Detección de Intrusión).
- Recopilar los datos necesarios (Sistema de métricas).
- Recopilar datos sobre el número de incidentes tratados y el tiempo empleado para su resolución.
- La Instrucción Técnica, obliga a las Entidades Locales a la comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito del ENS, para poder confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas. Para este fin el Centro Criptológico Nacional (CCN) ha desarrollado la herramienta INES (Informe Nacional del Estado de Seguridad) en donde todos los organismos públicos deben introducir sus datos de forma periódica (la herramienta está disponible en el portal del CCN-CERT.
- Para sistemas de categoría Alta se recopilará además datos para conocer la eficiencia del sistema de seguridad.

> Para su desarrollo nos servirá de base la a guía de seguridad (CCN-STIC-815) Métrica e indicadores, que define un conjunto ordenado de indicadores.

Medidas de Protección

Por último se presenta el conjunto de medidas que tienen como finalidad la protección de los activos concretos:

Protección de instalaciones:

Los equipos que gestionan la información, normalmente ubicados en una sala de acceso restringido, deberán de disponer de las adecuadas medidas de seguridad (Protección frente a incendios, energía eléctrica, control de acceso, etc.) En el caso de los Ayuntamientos de menor población o cuando se externalice el servicio, se deberá exigir a los proveedores que al menos cumplan las siguientes medidas de seguridad.

Gestión del personal:

Medidas conducentes a garantizar la seguridad de la información mediante una adecuada gestión del personal:

- Definir las responsabilidades, en materia de seguridad, de cada puesto de trabajo mediante la Caracterización del puesto de trabajo.
- Informar a cada persona que trabaje en el sistema de sus Deberes y obligaciones.
- Sensibilizar al personal respecto de su responsabilidad para la seguridad de los sistemas mediante la planificación de acciones de Concienciación para todo el personal y de Formación regular al personal en aquellas materias que requieran para el desempeño de sus funciones.
- En este caso, si la categoría de nuestro sistema sea ALTA también deberemos garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual mediante la provisión de Personal alternativo.

Protección de los equipos:

Conjunto de medidas que contribuyen a garantizar la seguridad de la información soportada por los equipos de los usuarios y la "depositada" en los puestos de trabajo estableciéndose normas para evitar que la información sea visionada o pueda ser sustraída por personal no autorizado como pueden ser la necesidad de mantener:

- Puesto de trabajo despejado, que implica que las mesas de trabajo deban estar despejadas de información al finalizar la jornada laboral, evitando que terceras personas no autorizadas puedan visualizar información, como por ejemplo el caso de empresas de limpieza. Esta medida es muy importante en zonas de acceso al público, como por ejemplo los servicios de atención ciudadana, donde un tercero no pueda llegar a ver información.
- Bloqueo del puesto de trabajo, preferiblemente de forma automática por el sistema superado un periodo razonable de actividad.
- Implementar medidas de seguridad que aseguren la Protección de portátiles que impidan, por ejemplo, que en caso de pérdida o robo no se acceda a la información que contiene en su interior.
- Disponer de Medios alternativos para el tratamiento de la información, debidamente configurados para su puesta en uso inmediato en caso de que fallen los habituales.

Protección comunicaciones:

Conjunto de medidas que garantizan la seguridad de la información en las comunicaciones fuera del propio dominio de seguridad:

- Utilización de un sistema de cortafuegos (Perímetro seguro) que separe la red interna de la exterior.
- Para la Protección de la confidencialidad y de la Protección de la autenticidad y de la integridad, deberán emplearse redes privadas virtuales (VPN) y se emplearán algoritmos de cifrado acreditados por Centro Criptológico Nacional (CCN).
- En caso de que el sistema alcance categoría ALTA, el sistema de cortafuegos deberá disponer de dos o más equipos redundados, en cascada y de diferente fabricante.

Además será necesario implementar medidas para acotar el acceso a la información y evitar la propagación de incidentes de seguridad mediante la ***Segregación de redes (Por ejemplo a través de una VLAN)*** y disponer de Medios alternativos de comunicación que garanticen un tiempo máximo de entrada en funcionamiento.

Protección de los soportes de información:

Conjunto de medidas con el objetivo de proteger los soportes de información:

» Etiquetado de soportes, indicando el nivel de seguridad de mayor calificación de la información que contienen, aplicando a los dispositivos removibles (CD, DVD, discos USB o similares).

» Garantizar la debida Custodia de estos soportes implementando medidas de control de acceso físicas y las relativas al mantenimiento (temperatura, humedad, etc.) especificadas por el fabricante.

» En cuanto al Transporte de estos soportes deberá mantenerse un registro de entrada y salida, así como mecanismos de criptografía, en caso de que información contenida así lo requiera.

» Cuando los soportes vayan a ser reutilizados o eliminados se aplicarán medidas de Borrado y destrucción segura.

» Si la información que contienen alcanza un nivel alto en Confidencialidad ([C]) o Integridad ([I], se emplearán mecanismos de criptográficos acreditados por el CCN y se emplearán Productos Certificados en los mecanismos de Criptografía.

Protección de las aplicaciones informáticas

Conjunto de medidas para la utilización de aplicaciones que aseguren la protección de la información. Esta medida está orientada a las Entidades Locales o empresas del sector privado que desarrollan aplicaciones, garantizando que las herramientas resultantes disponen de las correspondientes medidas de seguridad que permitan cumplir con el ENS:

» Implementar una metodología segura para el Desarrollo de aplicaciones, que también contemple como parte integral de su diseño medidas conducentes a garantizar la protección de la información: necesidad de implementar mecanismos de identificación y autenticación, qué mecanismos se deben implementar para proteger la información y las necesidades de logs (pistas de auditoría) y su tratamiento.

» Antes de la puesta en producción de las aplicaciones será necesario comprobar su correcto funcionamiento (Aceptación y puesta en servicio), mediante la realización de pruebas de seguridad, análisis de vulnerabilidades y pruebas de penetración.

» En caso de que el sistema alcance la categoría alta, también será necesario realizar un análisis de coherencia en la integración de los procesos y auditoría de código fuente.

En los procesos de licitación se deberá solicitar a las empresas que suministran o desarrollan aplicaciones la certificación de conformidad ENS en el ámbito del desarrollo seguro.

Protección de la información:

Conjunto de medidas para proteger la información independientemente del soporte en el que se encuentre.

» Cumplimiento en materia de protección de datos.

» Proceder a una Calificación de la información, redactándose los procedimientos que describan la forma en la cual se deberá etiquetar, el control de acceso requerido, su almacenamiento, copias de seguridad, etc. Si en la dimensión de Confidencialidad [C] se alcanza nivel alto, se deberán implementar mecanismos de Cifrado de la información.

» La Firma electrónica, deberá ser acorde a legislación vigente, los sistemas de firma electrónica avanzada estarán basados en certificados cualificados acreditados por el CCN, garantizándose la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa. En caso de que el nivel alcanzado para las dimensiones de Integridad [I] y Confidencialidad [I] sea alto, se usará una firma electrónica cualificada, se emplearán productos certificados, y se utilizarán Sellos de tiempo, para prevenir la posibilidad de repudio posterior.

» Los documentos deberán pasar también por un proceso de retirada de la información adicional contenida en campos ocultos, meta-datos, comentarios, revisiones, etc. especialmente cuando estos se vayan a difundir ampliamente (Limpieza de documentos). El estado ideal reside en que en los procesos de publicación en la página web las herramientas hagan una limpieza automática de metadatos.

Protección de los servicios:

Medidas para la protección de los servicios prestados:

- La ***Protección del correo electrónico (e-mail)*** de las amenazas que le son propias. Se trata de regular su uso mediante el establecimiento de normas, y crear una cultura de uso seguro a través de la formación y la concienciación.
- Medidas de ***Protección de servicios y aplicaciones web*** de las amenazas que le son propias, se utilizarán además "certificación de autenticación de sitio web" acordes a la normativa europea en la materia, implementando medidas preventivas y reactivas frente a ataques de denegación de servicio.
- En caso de que el nivel alcanzado para la dimensión de disponibilidad [D] sea alto además será necesario implementar un sistema de detección de este tipo de ataques y garantizar la existencia y disponibilidad de ***Medios alternativos***, para prestar los servicios en el caso de que fallen los medios habituales.

LOS SISTEMAS DE FIRMA ELECTRÓNICA AVANZADA ESTARÁN BASADOS EN CERTIFICADOS CUALIFICADOS ACREDITADOS POR EL CENTRO CRIPTOLÓGICO NACIONAL

3.1.3 [FASE 03] Conformidad con el ENS

1

Auditoría cada dos años

Preparación para conformidad

CCN-STIC-801 Responsabilidades y Funciones en el ENS
CCN-STIC-802 Auditoría del ENS
CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS

2

Alcanzar conformidad

Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad
Sector público, proveedores y prestadores de servicios de auditoría y certificación

CCN-STIC-809 Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento

3

Sistemas de categoría Básica

Autoevaluación de conformidad
Auditoría formal (recomendable)
Publicación en sede electrónica

4

Sistemas de categoría Media o Alta

Auditoría formal (obligatoria)
Publicación en sede electrónica

Objetivo

Obtener el distintivo que verifique la conformidad de implantación del ENS para el sistema/los sistemas de información. Para dar cumplimiento al artículo 41 del Real Decreto ENS, a la exigencia de dar publicidad de conformidad:

"Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad"

Distintivo de conformidad con el ENS

Descripción general

Alcanzar la conformidad con lo dispuesto en el Real Decreto Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, mediante la implantación de las medidas de seguridad recogidas en el anexo II, en función de la categoría alcanza por el sistema/los sistemas a proteger, mediante la obtención del distintivo de conformidad conforme a los criterios y procedimientos establecidos en la "Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad".

Guía de referencia general

- 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 ENS.

Guía CCN-STIC-809 Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento.

Principales tareas

El procedimiento para la determinación y declaración de la conformidad variará en función de la categoría del/los sistema/s:

- Sistemas de categoría BÁSICA: para determinar la conformidad bastará con una autoevaluación de conformidad, que verifique el cumplimiento del ENS. No obstante, sería recomendable someterse igualmente a un proceso de auditoria formal.

- La declaración de conformidad podrá ser expedida por la propia Administración se completará mediante un Distintivo de Declaración de Conformidad cuyo uso estará condicionado a la antedicha Declaración de Conformidad y serán acordes a lo establecido en la mencionada Instrucción Técnica; se publicará en la sede electrónica incluirá un enlace al documento de Declaración de Conformidad correspondiente.

- Sistemas de **categoría MEDIA o ALTA**: para determinar la conformidad, será necesaria la realización de una **auditoría formal de certificación de conformidad**.

- La certificación de conformidad tendrá que ser 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 y serán acordes a lo establecido en la mencionada Instrucción Técnica; se publicará en la sede electrónica e incluirá una enlace al a documento de Declaración de Conformidad correspondiente.

La determinación de la evaluación, así como la auditoría formal de conformidad con el ENS se realizará conforme a lo establecido en el artículo 34 ENS y el anexo III del ENS, y será realizada con periodicidad bienal.

Como ya se indicó anteriormente y tal como se establece en la Instrucción Técnica, en el apartado "VII. Soluciones y servicios prestados por el sector privado":

"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".

3.14 [FASE 04] Puesta en marcha del sistema de mejora continúa

1 Tareas de seguimiento

Procedimientos de control
Revisión de eficacia
Indicadores y métricas
Análisis de riesgos periódicos
Controles internos de cumplimiento
Auditorías de cumplimiento

CCN-STIC 815 Métricas e Indicadores
CCN-STIC 824 Informe Nacional del Estado de Seguridad
CCN-STIC 825 Certificaciones 27001

UNE-ISO/IEC 27001 Sistemas de Gestión de la Información (SGSI)
UNE-ISO 31000 Gestión del Riesgo
ISO 22301: Gestión de la Continuidad de Negocio

ens Esquema Nacional de Seguridad

2 Tareas de mejora

Implantar mejoras identificadas
Establecer acciones correctivas
Determinar acciones preventivas

3 Ciclo Deming

Planificar (P): realizar plan de adecuación
Hacer (D): implementar el ENS
Verificar (C): chequear la implantación
Actuar (A): subsanar desviaciones

Herramienta Clara (auditoría de cumplimiento con el ENS en Sistemas Windows)

CCN-STIC 825 Certificaciones 27001
UNE-ISO/IEC 27001 Sistemas de Gestión de la Información (SGSI)

Objetivo

Implementar un proceso integral de seguridad (al artículo 26 del ENS "Mejora continua del proceso de seguridad"), mediante la actualización y mejora continua. Obtener un Sistema de Gestión de la Seguridad de la Información conforme a la normativa ENS, basado en un ciclo de mejora continua (Ciclo de Deming)

Descripción general

Aplicar criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de la información mediante la implantación de un proceso de gestión de la seguridad de la información basado en un ciclo de mejora continua, conocido como Ciclo de Deming PDCA: Planificar (P=Plan), Hacer (D=Do), Verificar (C=Check) y Actuar (A=Act).

Descripción general

Guías de Seguridad CCN-STIC-815 relativa a métricas e indicadores y Guía de Seguridad CCN-STIC 825 sobre certificaciones ISO 27001.

- Estándares de seguridad:
  - » UNE-ISO/IEC 27001 Sistemas de Gestión de la Información (SGSI)
  - » UNE-ISO 31000 Gestión del Riesgo
  - » ISO 22301 Gestión de la Continuidad de Negocio

Principales Tareas

El proceso de mejora continua se lleva a cabo mediante la realización de iteraciones del ciclo de Deming:

- Planificar (P): realizar el Plan de Adecuación
- Hacer (D): implementar el ENS: llevar a cabo la implantación de las medidas de seguridad
- Verificar (C):
  - » Chequear la implantación mediante la declaración o certificación de conformidad con el ENS, según sea el caso.
  - » Establecimiento de métricas e indicadores para evaluar la eficacia de las medidas de seguridad implementadas.
  - » Actuar (A): subsanar las desviaciones encontradas en el punto anterior.

Como complemento a lo establecido en el ENS, para implementar el ciclo de mejora continua, se puede tomar como referencia estándares internacionales como puede ser la Norma ISO 27001 utilizada para implementar sistemas de gestión de la seguridad de la información.

La Guía CCN-STIC 825 relativa a las Certificaciones 27001, del CCN, nos proporciona un esquema de paralelismos entre una norma y otra. Para la gestión de los riesgos nos podemos apoyar en la norma ISO 3100 y para aquellos sistemas que alcance una categoría alta la norma ISO 22301 de gestión de la continuidad de negocio.

4 Sistemas de medición

Lo que no se mide, no se puede mejorar
Peter F. Drucker

4.1 Métricas e Indicadores

Cuando se pretende analizar, aprender y mejorar, es prácticamente imposible escaparse de los procesos de clasificación y medición. Los procesos de medición y clasificación generan datos. Los cuales pueden tratarse de diferentes maneras para obtener una visión más elaborada, bien sea resaltando algunas características, agregando datos de diferentes formas, o estudiando su evolución. Bajo el nombre genérico de métricas se recogen estos métodos de tratamiento para extraer información relevante de los datos disponibles. Un dato se convierte en indicador cuando es significativo para reflejar de forma concisa el estado de algo que nos preocupa.

En materia de seguridad de la información, ante la avalancha de datos disponibles, es conveniente resumir en unos pocos indicadores que sean suficientemente representativos de la seguridad del sistema, sin perjuicio de poder profundizar en más detalle (aplicando nuevas métricas a los datos primigenios).

Las definiciones que siguen están tomadas del trabajo de Debra S. Herrmann, citado en las referencias. No pretendemos ser escrupulosamente academicistas, pero sí entender qué datos necesitamos, qué unidades precisamos y qué métodos aplicamos para medir o clasificarlos.

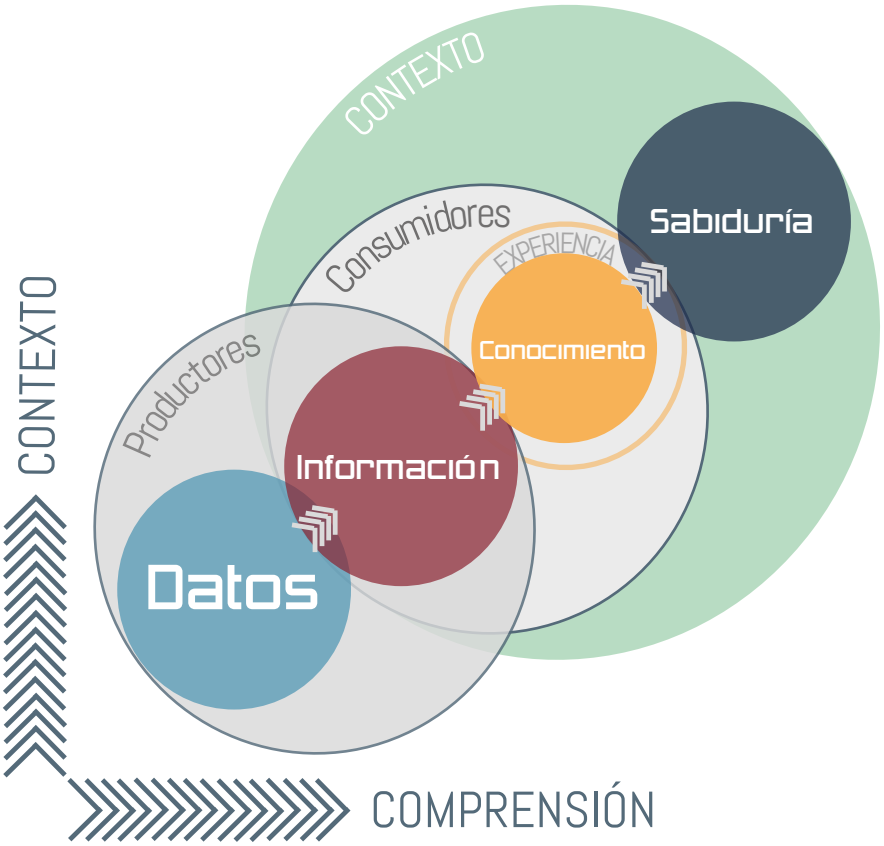
- **Datos**. Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesado automático.
- **Medición**. (1) Proceso que permite asignar números o símbolos a entidades de forma que nos permitan describirlas de acuerdo a unas reglas claramente definidas. (2) Comparación de la propiedad de un objeto con una propiedad similar en otro objeto que se usa de referencia.
- **Medida**. El número o símbolo asignado a una entidad como resultado de un proceso de medición. La medida sirve para caracterizar un atributo de la entidad.
- **Métrica**. Por una parte, es una unidad de medida (como lo es, por ejemplo, el sistema métrico decimal). Por otra parte, suele tener una finalidad, entendiéndose como una herramienta para entender la realidad y tomar decisiones al respecto. En este documento lo interpretaremos más bien en el segundo sentido.
- **Indicador**. (1) Instrumento que se utiliza para monitorizar la operación de un ingenio, en sentido general. (2) Química. Un elemento que cambia de color o estructura cuando se dan ciertas circunstancias, sirviendo como mecanismo de detección. (3) Economía. Conjunto de estadísticos que sirven para saber cómo está y a dónde se encamina la economía.
- **Cuadro de mando**. Conjunto de indicadores para resumir el desempeño de un sistema.

Esta guía establece unas pautas de carácter general aplicables a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas particulares. Se espera que cada organización pueda adaptarlas a su entorno particular.

Principales objetivos de la guía

- Proponer un conjunto de datos a registrar del sistema de información con el objetivo de establecer métricas posteriormente. Tanto locales –del sistema- como del conjunto de la Administración.
- Proponer un conjunto reducido de métricas o indicadores para caracterizar la posición del sistema de información en materia de seguridad.
- Proponer un conjunto de métricas o indicadores que permitan hacer un reporte anual, requerido por el artículo 35 del ENS.
- Proponer cuadros de mando para escenarios típicos.
- Establecer las pautas para que cada organismo extienda los indicadores que convengan en cada momento a sus necesidades.

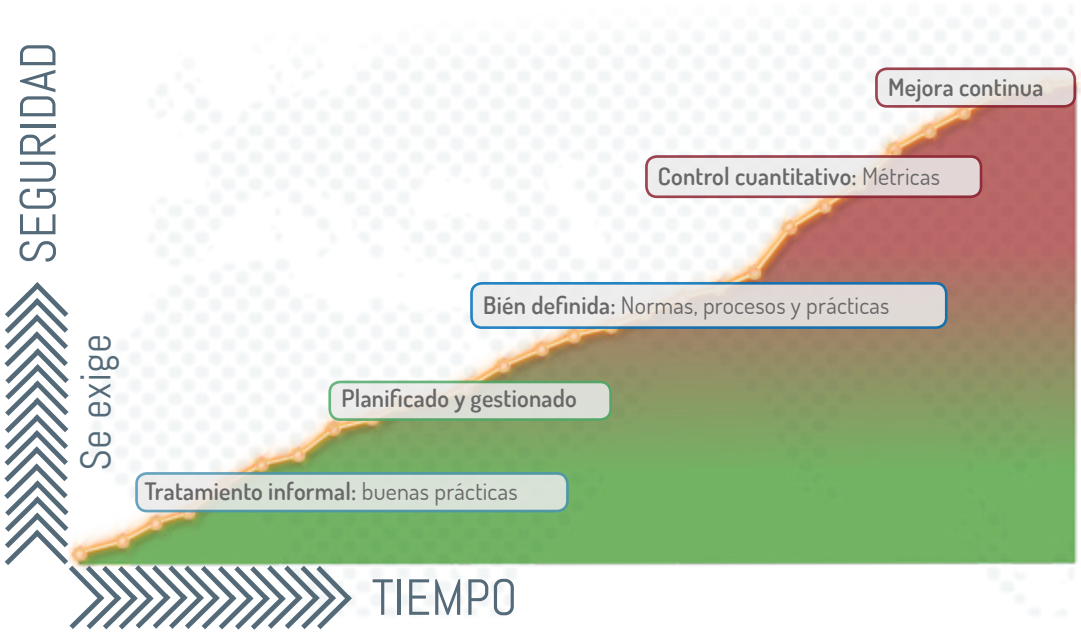
Es importante resaltar que los indicadores son herramientas para sustentar la toma de decisiones, especialmente en dos aspectos: (1) cumplimiento normativo y (2) ejecución de proyectos. Los aspectos de cumplimiento son relativamente estáticos, porque referencian un Real Decreto. En cambio, los proyectos son circunstanciales. De cada organismo y en cada momento, por lo que no pueden generalizarse. No obstante, se describe cómo desarrollar indicadores más específicos. Esperamos que el amplio conjunto de indicadores del anexo pueda ser reutilizado con frecuencia.



4.2 | Medición de la seguridad

La seguridad es una preocupación constante, cuando no creciente, tanto para los técnicos a cargo de los sistemas, como para los gestores de la organización. La seguridad técnica de los sistemas es un requisito indispensable; pero más allá de la técnica, los gestores necesitan tener confianza en que el sistema de información permitirá alcanzar los objetivos propuestos y establecer relaciones fructíferas con otras organizaciones. En este contexto, las métricas aparecen como necesarias para conocer el estado actual de la seguridad, mejorarlo y gestionar gastos e inversiones. Se requiere un eficaz alineamiento de los diferentes actores, tanto verticalmente (dentro de la propia organización) como horizontalmente (con otras organizaciones conectadas).

Es difícil analizar sobre el papel la seguridad efectiva de un sistema aislado; pero lo es aún más predecir la seguridad de dos sistemas si se interconectan. Los defectos de seguridad pueden afectar más o menos a un sistema aislado; pero presentan una desagradable tendencia a magnificarse cuando unos sistemas se interconectan con otros y pequeños desencuentros tienen consecuencias críticas.



¿Por qué queremos medir la seguridad?

Por varias razones:

- Lo que no se mide no se puede gestionar. Sería conducir a ciegas pretender llevar a cabo una actividad sin concretar objetivos y sin medir si nos vamos acercando a ellos, o no.
- Saber si está funcionando la seguridad. No puede ser que tras tantos recursos humanos y económicos dedicados a proteger la información y los servicios, no tengamos una realimentación de lo que hemos conseguido. Y esto conviene saberlo antes de que un incidente, o un desastre, nos ponga violentamente en la realidad.
- ¿Estamos mejorando adecuadamente? Cuando analizamos un sistema de información y proponemos mejoras de seguridad, invertimos en un proyecto que consume recursos, proyecto que debe gestionarse y que debe incluir indicadores de progreso, tanto de las etapas realizadas como de los objetivos alcanzados.
- El problema en cada momento es alcanzar los objetivos inmediatos y los indicadores deben permitir si estamos progresando según lo previsto hacia el objetivo deseado. O si vamos adelantados, o atrasados, o va a ser enteramente imposible llegar a donde se pretende en plazo y formas. Cuando los proyectos se expanden en plazos prolongados (años) los indicadores deben dar señales inmediatas de las desviaciones, mientras sea posible reaccionar con el mínimo esfuerzo extra.

Una metodología sencilla para lograr un buen nivel de seguridad. La seguridad de un sistema de información tiene tantas facetas que es fácil olvidar alguna. Por otra parte muchas facetas de la seguridad se describen con palabras, a menudo con objetivos negativos (que no ocurra tal cosa). Todo ello hace difícil marcarse unos objetivos de forma constructiva. Un buen conjunto de indicadores simplifica las reglas de forma radical:

HAY QUE LLEVAR TODOS LOS INDICADORES A LA ZONA VERDE

Al tiempo hay que ser conscientes de que un mal indicador puede hacernos errar completamente en nuestras decisiones y confundirnos respecto de dónde estamos realmente en materia de seguridad.

El poder medir la seguridad de un sistema de información permite llevar a cabo una serie de actividades de gestión:

» Tomar decisiones, tanto técnicas como de adjudicación de recursos

» Valorar la eficacia y eficiencia de la arquitectura de seguridad desplegada

» Facilitar la rendición de cuentas (accountability) de los responsables

Todo lo anterior se resume bajo el epígrafe de **permitir la gobernabilidad de la seguridad del sistema de información**.

4.2.1 Datos

Los sistemas de información son capaces de suministrar millones de detalles siempre y cuando se les requiera con anterioridad. Hay que saber lo que se necesita para apuntarlo cuando se sabe (después ya es tarde) y hay que saber lo que no se necesita para poder desecharlo. O, algo intermedio, saber qué necesitamos durante cuánto tiempo de forma que los registros de actividad (logs) no nos desborden y el sistema dedique su actividad a su propia medición antes que su misión última. En la práctica hay que:

- Decidir de antemano que vamos a registrar
- Establecer un plan de destrucción progresiva de logs
- En cada destrucción, guardar parte de la información, bien en bruto, bien consolidada
- Automatizar todo el proceso de captura y gestión de logs para prevenir errores humanos, olvidos y ataques intencionados

La recolección de datos es mecánica; pero la decisión de qué se mide y qué se conserva durante cuánto tiempo debe hacerse con un objetivo. Los objetivos los marcan, en última instancia, las necesidades del servicio para gestionarlo en sus diferentes niveles de responsabilidad.

4.2.2 Medidas

Los datos, en bruto, son poco relevantes. Desde cualquier punto de vista, la información atomizada es irrelevante. La información pasa a ser interesante cuando se mide (clasifica) y sobre todo cuando se agrega.

Cuando los datos se analizan utilizando algún criterio de evaluación, obtenemos una medida. Se dice que medimos. Las medidas quedan definida por una serie de valores de referencia (o unidades) y un algoritmo para deducir la medida a partir de los datos. Así, por ejemplo, para medir longitudes utilizamos el Sistema Métrico Decimal.

Hay medidas de varios tipos.

- Cuantitativas. Típicamente usan un número real que representa la proporción entre el atributo en el objeto medido y una referencia. Por ejemplo, una caja que mide 10 cm nos dice que es 10 veces la referencia que hemos acordado como centímetro.
- Cualitativas ordenadas. Típicamente rangos. Son como varios cajones en donde vamos metiendo los objetos medidos siguiendo algún criterio, cajones con la característica de estar ordenados. Por ejemplo, el Anexo I del ENS introduce los niveles BAJO, MEDIO y ALTO para clasificar las necesidades de seguridad.
- Cualitativas. Típicamente clasificaciones sin orden jerárquico. Por ejemplo, se puede saber cuánta gente va vestida de rojo, de amarillo..., sin que un color sea superior a otro.

Las medidas permiten estructurar la información y prepararla para un tratamiento, sea este analítico, estadístico, o descriptivo.

4.2.3 Métricas

Las métricas permiten a los responsables interpretar lo que ocurre. A los más técnicos les permite controlar el comportamiento de los sistemas; a los menos técnicos les permite escudriñar el alineamiento de recursos dedicados y resultados obtenidos.
Una buena métrica debe satisfacer algunos criterios básicos de calidad:

- Debe estar claro cómo se calcula a partir de los datos en bruto; si dos aplicaciones diferentes aplican la misma métrica de los mismos datos, el resultado de ambos procesos debería ser equivalente
- Debe estar claro cuándo (y cada cuánto tiempo) se mide, de forma que desviaciones u oscilaciones rutinarias no oculten desviaciones o comportamientos que denoten un problema

Las métricas suelen representarse gráficamente, mostrando su evolución en el tiempo; se necesitan reglas para interpretar el significado de los cambios, ¿cuánto es excesivo? ¿Cuánto es demasiado poco? ¿Es buena la estabilidad? ¿Qué significan los picos? ¿Y las variaciones abruptas? Y así un largo etcétera que permita entender el sistema observando la evolución de sus medidas.

Para que sea útil, una métrica debe estar bien (formalmente) definida, estando escrita la respuesta a las preguntas de los párrafos anteriores. Es más, desde un punto de vista de buena organización, debe estar claro quién es el responsable de su especificación, de su mantenimiento, elaboración regular, custodia de sus datos históricos, gestión de cambios y de la resolución de incidencias.

4.24 Indicadores

Sin duda los indicadores son importantes y podríamos definir cientos de ellos para cada sistema o subsistema funcionando en una institución, lo que hace francamente complicada la labor de valoración de los ingenieros o técnicos de sistemas.

Sin embargo es posible sin entrar en detalles, definir los indicadores precisos sobre sistemas consolidados, que permita a los ayuntamientos analizar el estado general de sus sistemas.
Necesitamos unos pocos indicadores que resumen la salud de la organización; pero al tiempo que se adapten a la situación presente. Además, cuando aparece un nuevo indicador en escena, los usuarios no esperan pacientemente a ver cómo evoluciona para aprender a interpretarlo: desde el primer día necesitamos ver cómo hubiera lucido el nuevo indicador en el pasado inmediato. Esto se consigue conservando las series históricas de medidas, lo que permite evaluar los nuevos indicadores sobre los datos del pasado inmediato.

Necesitaremos una serie de indicadores predictivos, para anticipar problemas y tomar decisiones sobre síntomas antes de que lleguemos al desastre. Decimos que estos indicadores fallan cuando son incapaces de prevenir un desastre, cuando no perciben los síntomas y, por tanto, no alertan al responsable que debe actuar.

> A menudo es difícil saber qué es una métrica o un indicador. Por ello los trataremos a la par en lo que sigue.

4.2.5 Tipos de métricas e indicadores

Métricas o indicadores pueden calificarse según los siguientes grupos, no necesariamente excluyentes:

De cumplimiento

Se busca conocer el grado de cobertura de una cierta referencia, que puede ser una política interna, un reglamento, un perfil, etc.

Suelen ser indicadores que miden si se han cumplido los requisitos formales o si se han tomado medidas preventivas. Un buen cumplimiento no garantiza el éxito del sistema frente a un ataque o un incidente, pero sí que el sistema esté mejor posicionado para afrontarlos.

Un mal resultado en estos indicadores es una señal de posibles problemas: caso de ataque o incidente, no estamos todo lo preparados que debiéramos.

De eficacia

Buscamos conocer el desempeño de una cierta función, desde el punto de vista de en qué medida logramos los resultados apetecidos.

En materia de seguridad, estos indicadores suelen tomar datos de los registros de incidencias, calibrando qué ha ocurrido y cómo hemos reaccionado.

Un mal resultado en los indicadores de hechos ocurridos descubre, tarde, que tenemos un problema con las medidas preventivas, y sugiere que deberíamos mejorar estas.

Un mal resultado en los indicadores que miden la calidad de la respuesta indica que el sistema necesita mejorar sus procedimientos, bien en alcance o en eficacia.

De eficiencia

Buscamos conocer el desempeño de una cierta función, desde el punto de vista de si el consumo de recursos está proporcionado a los resultados obtenidos.

Cuando el sistema es poco eficiente, se buscarán formas más eficientes de alcanzar los mismos objetivos de eficacia. A menudo se persiguen criterios de proporcionalidad ajustando la eficacia y la eficiencia hasta encontrarnos en un punto razonable.

De impacto

Se busca traducir los incidentes técnicos en consecuencias para la misión última del sistema: protección de una cierta información y prestación de unos determinados servicios.

Estos indicadores son los que suelen trasladarse a los órganos de gobierno para que tomen decisiones sobre la misión del organismo, sin entrar en los detalles técnicos.

Predictivos *(lead indicators)*

Se dice de los indicadores que anticipan lo que va a pasar. Es decir, no miden el pasado, sino que predicen el futuro. Más técnicamente, son los que cambian antes de que tengamos un problema de seguridad. Son muy útiles para organizar las medidas de protección dinámicamente, adaptándonos a la situación.

Por ejemplo, un semáforo en naranja es un indicador que nos permite predecir que el semáforo se va a poner en rojo en poco tiempo. Un aumento del nivel de alcohol en la sangre es un indicador que predice unos reflejos lentos y, probablemente, un accidente.

Explicativos *(lagging indicators)*

Son los que miden el pasado. Son útiles para entender lo que ha ocurrido y poder reaccionar con conocimiento de causa.

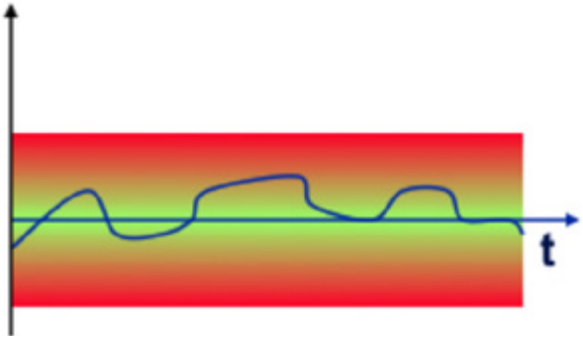
Por ejemplo, un suspenso es un indicador tardío de que no hemos estudiado lo suficiente. La fiebre es un indicador tardío de que estamos enfermos.

UN MAL RESULTADO EN LOS INDICADORES ES UNA SEÑAL DE POSIBLES PROBLEMAS: CASO DE ATAQUE O INCIDENTE, NO ESTAMOS TODO LO PREPARADOS QUE DEBIÉRAMOS

4.2.6 Explotación

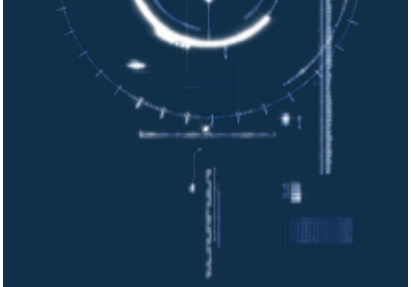
Las métricas y los indicadores hay que saber interpretarlos. Para ello se suelen aportar 3 elementos a su especificación:

- **Objetivo.** ¿Cuál es el valor objetivo? Dado que muchos indicadores son porcentajes, es habitual que se marquen objetivos como 100% de cumplimiento o 0% de incidentes.
- **Zona verde.** Se denomina así al rango de valores que se pueden considerar como suficientemente cercanos al objetivo como para no preocuparse.
- **Zona amarilla.** Se denomina así al rango de valores que caen fuera de la zona verde (más alejados del objetivo) y que deben ser investigados y corregidos.
- **Zona roja.** Se denomina así al rango de valores que caen más allá de la zona amarilla; tan alejada del objetivo que levantan las alarmas para que actuemos urgentemente.



No todas las medidas tienen líneas inferior y superior. Por ejemplo, las medidas de cumplimiento no tienen margen superior pues lo ideal es llegar al 100% y quedarse ahí; pero sí tendrán líneas inferiores.

NOTA: Los números son fáciles de calcular; incluso los modelos formales son fáciles de desarrollar. Pero la última palabra la tiene la cruda realidad. Es decir, el tiempo nos dará la experiencia para saber si un conjunto de métricas es más o menos adecuado como indicador de dónde estamos y qué va a pasarnos. Por ello el sistema de métricas e indicadores debe ser, a su vez, objeto de un proceso de mejora continua de la calidad.



EL SISTEMA DE MÉTRICAS E INDICADORES DEBE SER, A SU VEZ, OBJETO DE UN PROCESO DE MEJORA CONTINUA DE LA CALIDAD

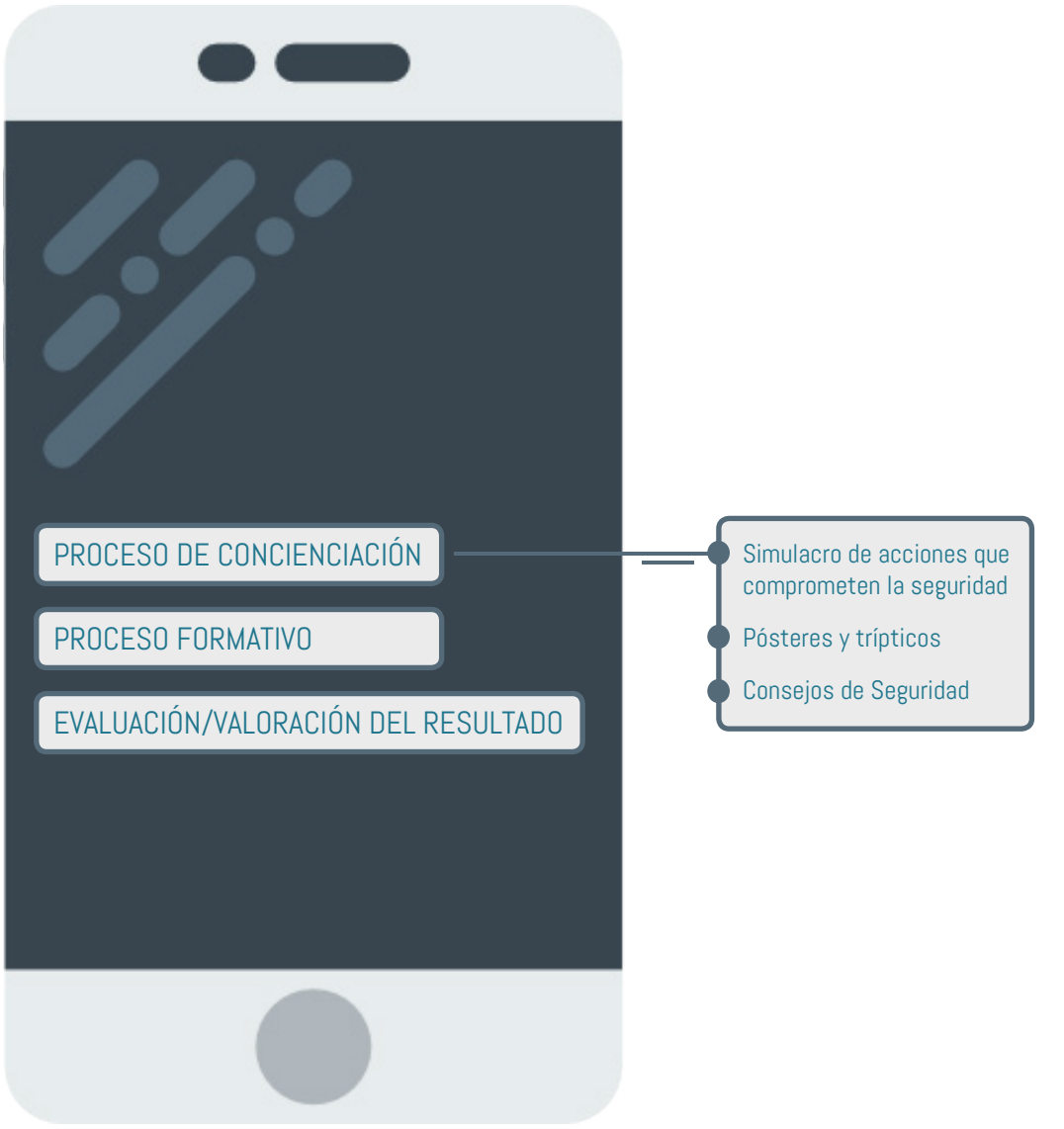
Por último, cabe recordar que a menudo manejamos el concepto de confianza, más allá del de seguridad. La confianza es una percepción subjetiva; pero en base a ella tomamos multitud de decisiones. La confianza crece con el tiempo: cada vez que el sistema se comporta como dicen (y predicen) las medidas. La confianza decae cada vez que las medidas yerran en su predicción o diagnóstico. En la medida en que los indicadores prevén los fallos, el sistema está bajo control; cada vez que una medida yerra en la predicción o mera detección, el sistema está fuera de control y el indicador bajo sospecha: hay que retirar la medida, o revisar la métrica o, simplemente, acompañarla de otras mediciones que, como colectivo, sean capaces de un mejor reporte de situación.

SON ÚTILES AQUELLOS INDICADORES QUE TIENEN LA CONFIANZA MERECIDA

> Ver Guía CCN-STIC-815 Métrica e Indicadores, que define un conjunto ordenado de indicadores.

5 Plan de Formación

Las entidades locales, o cualquier organismo público, deberían disponer de un plan de formación en el que se identifiquen las necesidades formativas de cada puesto de trabajo, así como la planificación en la impartición de la formación necesaria y la frecuencia con la que debe actualizar su formación. Deberá estar íntimamente ligado y coordinado con el **Plan de Concienciación**.



Con el objeto del desarrollo del Plan de Formación se establecerá un procedimiento documentado de gestión de la concienciación y formación que garantice la elaboración de un plan de formación anual donde se contemplen la identificación de las necesidades formativas en materia de seguridad así como la asignación de recursos y la programación de las acciones formativas a realizar.

Es recomendable consultar la existencia de Planes de Formación en materia de Seguridad a nivel Provincial, con el objeto de optimizar recursos y adherirse a los mismos. Otros organismos, como el CCN-CERT, INAP (Instituto Nacional de Administración Pública) e INCIBE (Instituto Nacional de Ciberseguridad de España), son fuente constante de actuaciones formativas y material en el que podemos basarnos e incluso participar.

Previamente a la definición y desarrollo del Plan de Formación, es esencial que se hayan ejecutado las siguientes acciones:

1. **Designación del responsable de la definición y puesta en marcha del Plan de Formación**. Es deseable un perfil directivo, de Recursos Humanos, con capacidad de tomas de decisión y asignación de recursos, tanto humano como material, a ser posible con conocimientos de Nuevas Tecnologías. Se coordinará con la Dirección en materia de Seguridad (Comité de Seguridad, Responsables de la Información, del Servicio, de la Seguridad y del Sistema)

2. **Adecuación a las siguientes medidas de protección:**

A. mp.per.1 Caracterización del puesto de trabajo.

B. mp.per.2 Deberes y obligaciones.

5.1 | Itinerario formativo

A la hora de desarrollar el Plan de Formación en materia de seguridad podemos seguir los siguientes pasos:

1. Análisis de la situación de inicio

Identificación de los destinatarios (debe ser integral, todos los puestos de trabajo) **y de las necesidades formativas de cada puesto de trabajo** (formación en materia de seguridad para el correcto desempeño de las funciones asignadas).

Asignación de recursos: presupuesto, recursos humanos, recursos materiales, comunicación, publicidad, etc.

2. Diseño del Plan de Formación

Elaboración de los contenidos formativos y programación de acciones formativas: objetivos, contenidos formativos, número de personas, cronograma, duración, jornada, modalidad (online/presencial), lugar de impartición, etc. Es importante establecer la **periodicidad en la ejecución de las actuaciones formativas** (anual, semestral, trimestral, etc.) como plan continuo de formación y tener en cuenta el análisis de situación de partida y los recursos asignados.

3. Ejecución del Plan de Formación

Se tendrá especial cuidado en el seguimiento de cada una de las acciones formativas, para poder evaluar el desempeño del plan de formación en el siguiente paso.

4. Evaluación/valoración del resultado

Se pretende medir el grado de adecuación entre objetivos y resultados formativos. Se evaluarán indicadores cuantitativos (ej. que definen el número de participantes o acciones formativas) o cualitativos (ej. elección de formadores o contenido de la formación). Se tendrá en cuenta, entre otros, la eficacia de la formación, la evaluación del aprendizaje, el retorno de la inversión, etc.

5. Plan de mejora o cambios

Sobre el Plan de Formación (puntos 1, 2, 3, 4) en base a la evaluación/valoración del resultado de la ejecución del mismo y sobre el Plan de Concienciación, si se detectasen.

- Análisis de la situacion de inicio
- Diseño del Plan de Formación
- Ejecución del Plan de Formación
- Evaluación/valoración del resultado
- Plan de mejora o cambios

Complementariamente al Plan de Formación Anual, se desarrollarán actuaciones de formación continuas dado que **"La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo"**.

Tanto el personal alternativo como el de nueva incorporación están sujetos a las mismas medidas de formación, concienciación, deberes y obligaciones que el personal habitual, por lo que se deberá prever su incorporación en el plan de formación y de concienciación continuo.

5.2 | Contenidos formativos mínimos

A la hora de elaborar los contenidos formativos se deben considerar actuaciones formativas relacionadas con:

- La clasificación y uso de información en soporte papel o soporte electrónico **(mp.per.4)**.
- Protección de equipos y sistemas operativos **(mp.per.4)**.
- Detección y reacción frente a incidentes, dando a conocer los procedimientos internos establecidos en esta materia y concienciando al personal sobre las situaciones de riesgo que conlleva el uso de las tecnologías de la información **(mp.per.4.)**.
- Situaciones extrañas, anómalas o circunstancias de riesgo que deban ser conocidas por los empleados y les permita la detección temprana de incidentes **(mp.per.3)**.
- Conocimiento de los procedimientos internos de notificación y gestión de incidentes **(mp.per.3)**.
- "Normas de uso de los sistemas de información de la Organización", en especial "Uso del correo electrónico" **(org.2. y mp.s.1)** y el uso de Internet.
- "Política de Seguridad" **(org.1)**

A la hora de elaborar los contenidos formativos es una buena práctica tener en cuenta estos tres posibles perfiles dentro de la organización:

- Dirección en materia de Seguridad (Comité de Seguridad, Responsables de la Información, del Servicio, de la Seguridad y del Sistema).
- Personal TIC y administradores de seguridad.
- Usuarios de los Sistemas de Información.

Tomando como referencia el Kit de Concienciación INCIBE, y desde un punto de vista más didáctico, los siguientes contenidos formativos ocupan un lugar importante:

- La información
- Los soportes
- El puesto de trabajo
- Dispositivos móviles

Como contenido transversal debemos considerar ejecutar actuaciones formativas relativas a la LOPD y Reglamento (UE) 2016/679

5.3 Difusión y acceso a contenidos

Como apoyo al desarrollo del Plan de Formación y como base para un plan de formación continuo, es interesante disponer de un medio de distribución de materiales y contenidos de forma electrónica (típicamente en forma de portal) para poner a disposición de los empleados diferentes recursos: presentaciones, documentos y manuales, tests, videos interactivos.

Una de las claves del éxito del Plan de Formación son las acciones de Publicidad y Comunicación del mismo a todos los agentes implicados. Descuidar estas acciones puede conllevar a resultados pobres o baja participación.

"La correcta gestión de la seguridad, depende de todos"
Virginia M.

5.4 Plan de sensibilización y concienciación

La Seguridad es una de las necesidades básicas que se debe cubrir en una institución.
Sin embargo, es un término que cada vez se complica más. En este momento tenemos que tener en cuenta la seguridad técnica, móvil y física y tomar conciencia corporativa de todas ellas.

La correcta gestión de la seguridad es una de las asignaturas pendientes, siendo uno de los aspectos fundamentales que debe tener en cuenta toda institución. Concienciar tanto a los trabajadores como a los usuarios potenciales de las herramientas de gestión y servicios públicos que se desarrollen, es una tarea fundamental.

Desde las administraciones, hay que concienciar y establecer una **cultura corporativa en política de seguridad** tanto teórica como práctica, a cada trabajador, y específica según sus conocimientos, y adaptada a las tareas que lleva a cabo diariamente en su puesto de trabajo.

Formación vs Concienciación

Hay que diferenciar entre concienciar y formar.

> **Concienciar:** Crear cultura de seguridad. Es necesario concienciar a todos los miembros de la institución en el uso de la seguridad y las implicaciones y riesgos de no asumirla.
>
> **Formar:** La formación es continua y no acaba nunca. Se debe involucrar a toda la organización, pero a diferencia de la concienciación, los cursos deben ser dirigidos.

Es por ello que en esta guía se trabajan dos apartados, por un lado el **Plan de Concienciación** y por otro el **Plan de Formación** e n seguridad.

5.4.1 Plan de Concienciación

En este apartado se incluyen algunas recomendaciones con las que se pretende concienciar a todos de que contar un **Plan de Concienciación en Seguridad debe constituir una parte central de la estrategia en seguridad** que vayamos a implementar.

La administración tiene que tener una estrategia que tenga por objetivo una concienciación de sus políticos/as y de sus técnicos/as para que respondan de forma ágil a las necesidades de una competencia cada vez más compleja en la materia de Seguridad, física y lógica.

Desgraciadamente, la seguridad total no existe. Aun así, es importante insistir y recordar:

- Que **cada administración tiene sus propias características** y que será necesario adaptar el Plan de concienciación a la realidad de nuestra Administración.
- Que las principales fisuras de seguridad suelen estar en nuestra propia organización. Por eso, es importante centrarnos en la visión interna.

Cualquier proceso interno supone un **cambio cultural** importante en la organización, por tanto será fundamental plantear un plan de concienciación interno que culturice al conjunto de la organización de la importancia y beneficios que implican la seguridad y su implicación en el proceso.

Cada organización tiene su propia estructura interna de funcionamiento. No obstante, es recomendable definir y pensar acciones de concienciación adecuadas a la **heterogeneidad de las personas** que forman parte de nuestra organización y al rol que puedan tener en materia de seguridad.

Recomendaciones:

Seguridad de la información es más que seguridad informática

La protección de la información se considera un gran reto en las organizaciones del siglo XXI. Uno de los principales aspectos recae en **concienciar a las personas que manejan la información**, ya que deben ser conocedoras tanto de los riesgos existentes como de las funciones y obligaciones que se pudiesen derivar de su actividad profesional.

«Una cadena es tan fuerte como su eslabón más débil»

Esta frase tan popular significa que aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si alguno de ellos, falla, toda la seguridad se ve comprometida.

Diversos estudios demuestran que **el usuario es un eslabón más de la cadena de seguridad**. Para cambiar esta situación, es necesario invertir también en la concienciación en seguridad a usuarios.

Es aquí la diferencia entre seguridad de la información y seguridad informática.

Estas acciones de concienciación buscarán una implicación de toda la organización, y que tendrán como principal objetivo, exponer los principales riesgos en materia de seguridad sobre personal no técnico, aspecto clave para que la organización interiorice los posibles cambios organizativos en materia de seguridad.

54.2 Propuesta Plan corporativo

El plan se desarrollará de forma **transversal** durante todo el ciclo de vida del proceso. Las acciones de concienciación **deberán ser presenciales** y como mejora, se aconseja complementar con acciones on-line.

Jornada concienciación para directivos (Equipo de gobierno)

Número de Sesiones: 1

Duración: 2-3 horas

Objetivo: Desarrollar los principales conceptos vinculados con la seguridad de la información, evitando los principales riesgos derivados del uso de nuevas tecnologías

Destinatarios: Equipo de Gobierno / personal directivo

Temas sobre los que trabajar:

- Conceptos generales sobre seguridad
- El Puesto de trabajo: Normas de conducta
- Gestión de contraseñas
- La ubicación de la información en los servicios en la nube. Herramientas permitidas.
- Técnicas de ingeniería social
- Prácticas adecuadas en el correo electrónico
- Uso seguro en el acceso a Internet y WIFI
- Instalación de software original.
- Amenazas y medidas de protección
- Utilización correcta de dispositivos USB
- Seguridad en dispositivos móviles y portátiles
- Programas de mensajería instantánea

Jornada formativa: Valoración de información y servicios

Número de Sesiones: a determinar según las características de la organización

Duración: deseable 5-8 horas

Objetivo: Conocer las Funciones y Obligaciones derivadas el ENS

Destinatarios: Responsables de la información y servicios

Temas sobre los que trabajar:

- La Administración Electrónica y la Seguridad de la Información. Implicaciones de las nuevas Leyes 39 y 40 de 2015
- Órganos y Organismos de referencia
- Los requisitos mínimos de Seguridad de Información
- Dimensiones de la seguridad
- Amenazas y vulnerabilidades
- Valoración de la información y servicios.
- Seguridad en dispositivos móviles y portátiles
- Programas de mensajería instantánea

Será deseable siempre que las sesiones presenciales se complementen mediante sesiones alternativas on-line, como mejora y refuerzo de concienciación.

Jornada formación técnica sobre análisis de riesgos

Número de Sesiones: a determinar según las características de la organización

Duración: 15-20 horas

Objetivo: Conocimiento sobre los Sistemas de Gestión de Seguridad de la Información conforme a la norma UNE-ISO/IEC 27001 (SGSI) e integración con el ENS.

Destinatarios: Personal IT del área de nuevas tecnologías/departamento de informática

Temas sobre los que trabajar:

- Introducción
- Organización de la Seguridad
- Identificación de activos dentro del alcance
- Análisis de Riesgos
- Gestión y tratamiento del riesgo
- Continuidad de Negocio
- Gestión documental asociada al SGSI
- Seguimiento del SGSI
- Paralelismo SGSI con ENS

Jornada concienciación general para el personal de la organización

Número de Sesiones: a determinar según las características de la organización

Duración: 4-5 horas (anualmente)

Objetivo: Desarrollar las pautas de seguridad necesarias para hacer un buen uso de la información y de los sistemas que la tratan, con el objetivo de que puedan ser conocidas y aplicadas por todos los usuarios/as y reducir la probabilidad de fallos y daños causados por problemas de seguridad

Destinatarios: Todo el personal de la organización. Realización de acciones sectoriales en función de la tipología de datos (Policía Local, Servicios Sociales, trabajo con menores de edad, redes sociales, etc.)

Temas sobre los que trabajar:

- Medidas de seguridad generales y específicas por puesto de trabajo
- Protección del puesto de trabajo
  - » Ordenadores personales y portátiles
  - » Equipos móviles
- Mecanismos de identificación y autenticación:
  - » Usuario y contraseña
  - » Biometría
  - » Tarjetas inteligentes
  - » Etc.
- Riesgos en el uso de dispositivos:
  - » Correo electrónico
  - » Internet
  - » Etc.
- Decálogo de seguridad

Es necesario volver a recordar que **no existen actuaciones milagrosas**. Como decíamos, ésta es una actividad que se valorará por la **perseverancia y continuidad**. Se trata de realizar, con cierta metodología, reuniones, acciones de concienciación tradicionales o innovadoras con los colectivos definidos, de forma constante y no sólo al inicio del proceso de cambio. La Agencia Española de Protección de Datos ha publicado en julio de 2017 el Esquema de Certificación para los DPD.

En el caso de tratamiento de datos de carácter personal, se deberá realizar un plan específico de adaptación ante la entrada en vigor del Reglamento Europeo (RGPD) así como acciones específicas de formación para el Delegado de Protección de Datos (DPD).

Cada administración deberá escoger las acciones que mejor se adapten a sus características y, siempre que sea posible, implicar en nuestra estrategia y diseño del Plan de Concienciación a los departamentos de prensa y de comunicación de la organización.

6 Plan de DIFUSIÓN

"Lo que no se enseña, no se conoce y no existe"
Pablo Bárcenas

El Plan de Difusión tiene como finalidad dar a conocer al conjunto de Entidades Locales Españolas el documento "Libro de Recomendaciones para el Itinerario de Adecuación al ENS para las Entidades Locales".

Esta publicación surge de la necesidad detectada por la Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias (FEMP), de ayudar a los Entes Locales, especialmente a aquellos que carecen de los conocimientos técnicos necesarios y facilitadores de la implantación del ENS.

Cobra por tanto especial relevancia, el diseño y ejecución de un Plan de Difusión que permita llegar con acierto a los lugares donde la demanda es más evidente, contando para ello con otros interlocutores conocedores de la realidad en cada uno de los territorios.

Por otra parte, la FEMP dispone de mecanismos de comunicación a través de los cuales será posible facilitar la información y la publicidad necesarias que el documento se merece.

Pero el Plan quedaría incompleto si no fuéramos capaces de realizar convocatorias presenciales, en las que exponer el alcance de la guía, resolver las dudas que puedan surgir, y realizar ejercicios prácticos que consoliden el conocimiento del ENS y que faciliten la elaboración de los participantes de su propio Itinerario en virtud de las condiciones en las que se pueda encontrar su Entidad.

De esta manera, nuestro Plan de Difusión se apoyará sobre tres pilares:

- ## Diputaciones Provinciales/Federaciones Territoriales:

Como socios prioritarios de esta Federación, y como conocedores de su realidad Territorial, solicitaremos su colaboración para realizar acciones de difusión que en su mayor parte tengan como destinatarios últimos a los municipios de menor población.

En especial, buscaremos la implicación de Diputaciones, Cabildos y Consejos Insulares, que tiene el mandato normativo de facilitar el desarrollo de la Administración Electrónica en municipios de su competencia menores de 20.000 habitantes, para que se involucren activamente en la implantación del ENS, facilitando el desarrollo de un itinerario factible en virtud de las características propias de cada ayuntamiento.

- ## Difusión a través de las herramientas de Comunicación FEMP:

» Correo electrónico

Se realizará el envío de la información al conjunto de Entidades Locales españolas, intentando personalizarla en el responsable del desarrollo de la e-Administración.

» Carta Local

Se publicará una noticia relacionada con el ENS y el trabajo desarrollado con el Libro Itinerario, en la Revista de la FEMP de edición mensual "Carta Local"

» Página Web de la FEMP

Se pondrán a disposición los contenidos desarrollados en la Página Web de la FEMP, en el apartado del Área de Sociedad de la información, para consulta y descarga, en su caso, por parte de los interesados. De igual forma, dicho contenido estará presente en el portal del CCN-CERT, del Centro Criptológico Nacional.

» 2.4.- Edición Impresa

Se buscarán alternativas y sponsors para poder contar con una mínima edición impresa del documento, que facilite su visibilidad en determinados entornos.

• Formación/Jornadas:

» Jornada de Presentación en la FEMP

Con cabida para técnicos de Entidades locales, pero a la que se invitará prioritariamente a los Cargos Electos, que deben liderar y propiciar el cambio en las Administraciones.

» Formación Continua

Se ha previsto, dentro del Plan de Formación Continua de la FEMP 2017, el desarrollo de una Acción Formativa, que gire en torno al ENS y la Guía elaborada, que contará con exposiciones sobre el caso teórico, Buenas experiencias de Entidades Locales que puedan servir de modelo a otras instituciones, y el desarrollo de casos prácticos de elaboración del Itinerario personal de cada Entidad Asistente.

Una segunda edición de dicha Acción formativa, será propuesta, a los responsables del Plan de Formación Continua de la FEMP 2018.

» Jornadas en Diputaciones/Federaciones Territoriales

Se facilitará un modelo de jornada al conjunto de Federaciones Territoriales, así como a las Diputaciones Provinciales, Cabildos y Consejos Insulares, para que puedan replicar acciones de formación en sus territorios, colaborando y coordinando las mismas en la medida de las necesidades y/o la demanda.

» Jornadas con otros Actores institucionales

Se buscará el apoyo del Centro Criptológico Nacional para que en su catálogo de formación, incluya una Acción basada en la Guía y destinada al conjunto de Entidades Locales Españolas.

» Jornadas con esponsorización

Se propiciará y buscarán alternativas para la realización de jornadas en la que puedan participar empresas que estén colaborando con Entidades Locales para facilitarles el cumplimiento del ENS, de manera que se visualicen para aquellos interesados que precisen de ayuda externa para conseguir sus objetivos.

» Otras Jornadas/Conferencias

Se buscará oportunidades para divulgar el trabajo en jornadas y conferencias desarrolladas por terceros, tales como las Jornadas del CCN-CERT 2017, CNIS 2018, etc.

Las actuaciones que deben implementarse se desarrollarán a partir del último trimestre de 2017, y se extenderán durante la mayor parte de 2018. Siguiendo la siguiente Cronología:

Actividad	Fecha
Correo divulgativo, artículo en carta Local y Publicación en Web FEMP	Primera quincena octubre 2017
Jornada de Presentación en la FEMP	Segunda quincena octubre 2107
Acción de Formación FEMP	Primera quincena noviembre 2017
Edición Impresa	Primera quincena diciembre 2017
Jornadas CCN-CERT	Primera quincena diciembre 2017
Jornada esponsorizada	Segunda quincena febrero 2018
Acción Formativa FEMP	Segunda quincena octubre 2018
Jornadas Diputaciones/Federaciones Territoriales	Durante 2018
Otras Jornadas/Conferencias	Durante 2018

SE HA PREVISTO, DENTRO DEL PLAN DE FORMACIÓN CONTINUA DE LA FEMP 2017, EL DESARROLLO DE UNA ACCIÓN FORMATIVA, QUE GIRE EN TORNO AL ENS

7

Crea tu propia Hoja de Ruta en Seguridad

Una hoja de ruta es un plan que establece a grandes rasgos la secuencia de pasos para alcanzar un objetivo. Puede entenderse como un plan de acción a corto, medio y largo plazo, y general que acerca los objetivos estratégicos a objetivos más tangibles y alcanzables.

La finalidad de la hoja de ruta es servir de base a la institución para saber dónde está y qué debe hacerse para llegar a donde se quiere. Todo ello con objeto de definir sus objetivos, así como ofrecer unas líneas estratégicas claras para el desarrollo de los distintos procesos en aras de alcanzar realmente esos objetivos.

Es un plan sobre una problemática concreta a tratar, a las que hay que dar una solución.
La seguridad actúa sobre procesos, personas y tecnología, y en esta guía estratégica de seguridad se presenta un Diagrama General por Fases en el marco de modelo práctico a seguir. En cada Fase se definen los pasos que hay que dar.

La combinación de esos pasos de cada Fase con los factores descriptivos de cada organización nos permitirá llegar a nuestra hoja de ruta en adecuación a la seguridad.

FASE 1: Desarrollo de un Plan de Adecuación ENS

PASO 1: Elaboración de una Política de Seguridad de la Información

PASO 2: Identificación de la información y los servicios. Determinación de la Categoría del Sistema.

PASO 3: El Análisis de Riesgos

PASO 4: La declaración de aplicabilidad (SoA)

PASO 5: El informe de insuficiencias (Gap Analysis)

PASO 6: El Plan de Mejora de la Seguridad (Plan de Tratamiento del Riesgo)

FASE 2: Implementación del Plan de Adecuación

TAREA 1: Marco Organizativo

TAREA 2: Marco Operacional

TAREA 3: Medidas de Protección

FASE 3: Conformidad con el Esquema Nacional de Seguridad

CATEGORÍA BÁSICA

CATEGORÍA MEDIA O ALTA

FASE 4 Puesta en marcha del sistema de mejora continúa

P: Planificar D: Hacer C: Verificar A: Actuar

> No hay dos hojas de ruta iguales.
> Las hojas de ruta se crean por cada organismo en base a un itinerario recomendado.

Anexos Tomo 1

ANEXO 1. Modelo pliego de prescripciones técnicas para la adecuación al ENS

El texto siguiente esboza un Modelo de Pliego de Prescripciones Técnicas para la Adecuación al ENS, y contiene una serie de pautas de carácter general que podrían usar las entidades locales a tal propósito, sin entrar en casuísticas particulares y sin pretender constituirse en un texto normativa o técnicamente cerrado. Se espera que cada entidad lo particularice para adaptarlo a su problemática concreta y a las regulaciones que en cada momento y lugar resulten aplicables.

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE REGIRÁN LA EJECUCIÓN DEL CONTRATO DE SERVICIO DE ASISTENCIA TÉCNICA EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN EL MARCO DEL ESQUEMA NACIONAL DE SEGURIDAD PARA <<LA ENTIDAD LOCAL>>

PRIMERA.- Objeto del contrato

El presente pliego tiene por objeto establecer las condiciones generales y las características técnicas que deberán cumplirse para la contratación de los servicios de asistencia técnica en materia de seguridad de la información, en el marco del Esquema Nacional de Seguridad para <<LA ENTIDAD LOCAL>>, que comprenden los servicios necesarios encaminados hacia la adecuación y cumplimiento de <<LA ENTIDAD LOCAL>> del Esquema Nacional de Seguridad (RD 3/2010, de 8 de enero).

SEGUNDA.- Antecedentes

El Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, tiene por objeto establecer una política de seguridad en la utilización de los medios electrónicos y está constituido por una serie de principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Es decir, el ENS dispone la obligatoriedad de implantar, a las Administraciones Públicas que ofrezcan Servicios de Administración Electrónica, de sistemas de seguridad de la información.

<<LA ENTIDAD LOCAL>> en la implementación de los sistemas TIC (Tecnología de la Información y la Comunicación)debe cumplir los diferentes marcos normativos relacionados con las TIC, de manera que se garantice la confianza en el uso de los medios electrónicos por parte de los ciudadanos.

En base a estos criterios, el objetivo de esta contratación se dirige hacia la adecuación de <<LA ENTIDAD LOCAL>> respecto de estas obligaciones, aportando con ello la necesaria cobertura jurídica, organizativa y técnica requerida para cimentar las garantías que deben sustentar estas nuevas formas de relación entre <<LA ENTIDAD LOCAL>> y Ciudadanos.

TERCERA.- Definición, contenido y condiciones de ejecución de los trabajos

Los servicios en relación a la ejecución del contrato comprenden los trabajos relacionados con el Esquema Nacional Seguridad (RD 3/2010 de 8 de enero, ENS en adelante), en concreto: Servicio de adecuación al ENS con la elaboración del Plan de Adecuación al ENS, que incluirá como mínimo:

1. Diagnóstico de la situación actual del Sistema para determinar el grado de cumplimiento de las medidas establecidas en el ENS.
2. Desarrollo completo del Plan de Adecuación al Esquema Nacional de Seguridad, contemplando todas las actividades y entregables incluidos en la Guía CCN-STIC 806 vigente, como son:

    a. Revisión de la Política de Seguridad actual, y en su caso, verificación del contenido, para que sea acorde a lo establecido en el RD del ENS.

    b. Determinación de la categoría del sistema.

    c. Realización de un análisis de riesgos, acorde a lo establecido en el Anexo II del Real Decreto ENS, utilizando la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas) y la herramienta para el análisis de riesgos PILAR.

    d. Elaboración de la Declaración de Aplicabilidad.

    e. Elaboración del Informe de insuficiencias del sistema.

    f. Elaboración del Plan de mejora de la seguridad.

    g. Identificación y análisis de Interconexiones con otros sistemas para la prestación de los servicios.

3. Servicios de formación al personal de <<LA ENTIDAD LOCAL>>, que incluyan la formación a diferentes perfiles de usuarios (alta dirección, responsables de información y servicios, técnicos y usuarios), en relación a la Seguridad de la Información, así como en las herramientas utilizadas para el desarrollo del proyecto (análisis de riesgos y herramienta de análisis, dirigidas al perfil técnico). La formación se impartirá en las dependencias de <<LA ENTIDAD LOCAL>>, en las fechas y horarios que determine <<LA ENTIDAD LOCAL>>. La formación incluirá como mínimo los siguientes cursos:

   - Perfil Alta Dirección: 1 curso (de 2 horas de duración).
   - Perfil Responsable de Información y Servicios: 2 cursos (de 3 horas de duración).
   - Perfil Técnico: 1 curso (de 3 horas de duración).
   - Perfil Usuarios: 8 cursos (de 1 hora de duración).

Durante la ejecución de los trabajos objeto del contrato la empresa adjudicataria se compromete a facilitar a la <<ENTIDAD LOCAL>> la información y documentación que solicite a efectos de conocer las circunstancias en que se desarrollan los trabajos, así como los problemas que puedan plantearse y las tecnologías, métodos y herramientas para resolverlos.

CUARTA.- Dirección e inspección de los trabajos

La dirección del proyecto por parte de <<LA ENTIDAD LOCAL>> recaerá conjuntamente en el Secretario General y el Jefe de Sistemas de Información y/o personas en quien deleguen, que supervisarán la ejecución de los trabajos y la coordinación entre el equipo del proyecto y el personal de <<LA ENTIDAD LOCAL>>. Estos trabajos comprenderán:

- Dirigir y supervisar la realización y el desarrollo de los trabajos y el cumplimiento de plan de trabajo.
- Aprobar los documentos que se elaboren.
- Intervenir para la implicación del personal de <<LA ENTIDAD LOCAL>>, junto con la empresa contratada, en el desarrollo de aquellos trabajos, que así lo requieran.

Como mínimo mensualmente se realizarán reuniones de coordinación, supervisión y seguimiento. Se realizará una presentación, previa al comienzo de los trabajos, al Comité de Seguridad de las Tecnologías de la Información y la Comunicación de <<LA ENTIDAD LOCAL>>, otra presentación a la mitad del proyecto y una última presentación a la finalización del mismo.

QUINTA.- Solvencia técnica empresarial y Equipo técnico

El licitador deberá acreditar la prestación de servicios de similares características e importes en los últimos N años.

El licitador deberá presentar el equipo del proyecto, quienes deberán acreditar formación en Derecho Administrativo de aplicación, Esquema Nacional de Seguridad y seguridad de la información, con perfiles técnicos y jurídicos.

<En función del alcance del proyecto se podrán exigir diferentes certificaciones, tanto al equipo de trabajo (CISA, CISM, etc.) o bien la certificación de conformidad de la empresa, en categoría BÁSICA o MEDIA, estableciendo que su alcance está en la prestación del servicio. >

SEXTA.- Lugar de realización de los trabajos

Las reuniones/sesiones necesarias para la ejecución y seguimiento del proyecto, así como las sesiones de formación, se llevarán a cabo en las dependencias municipales de <<LA ENTIDAD LOCAL>>.

SÉPTIMA.- Presentación de ofertas

La propuesta técnica incluirá, en orden, los aparatados indicados a continuación. Así mismo, como anexos, se podrán incluir aquellos puntos que se consideren oportunos:

1. Objeto y alcance la propuesta.
2. Metodologías a aplicar para la realización de los trabajos.
3. Planificación detallada de los trabajos a realizar, en relación a los tres servicios solicitados, con la asignación de las personas responsables de su ejecución, jornadas a realizar, indicación de las herramientas a utilizar (si es de aplicación) y relación de los productos a obtener en cada uno de ellos (si es de aplicación).
4. Actuaciones adicionales (mejoras a la oferta técnica) incluidas en relación al ENS.
5. Acciones de formación dirigidas al personal de <<LA ENTIDAD LOCAL>>, con indicación de los diferentes perfiles a formar, cursos/horas dedicados a cada uno de ellos, contenidos a impartir y material proporcionado.
6. Relación de trabajos realizados por la empresa en relación al Esquema Nacional de Seguridad.
7. Presentación del equipo de trabajo asignado al proyecto. Se incluirá el currículum de los miembros del equipo de trabajo, con sus méritos y con los certificados de los conocimientos y experiencia requeridos.
8. Propuesta económica.
9. Anexos.

OCTAVA.- Criterios de valoración de ofertas

Los criterios que se aplicarán para la adjudicación del contrato serán los siguientes:

- Proposición técnica
- Mejoras a la oferta técnica
- Actividades de formación
- Proposición económica

En los contratos de prestación de servicios el precio no debería ser un valor determinante ya que los servicios dependen de la cualificación del equipo de trabajo. Los trabajos de seguridad de la información requieren la contratación de empresas y profesionales especializados en el sector.

La forma de evaluar los criterios será la siguiente:

La Mejor proposición técnica. Se valorará:

- La metodología aportada para la ejecución del servicio.
- La adecuación de los trabajos a las Guías de Seguridad del Centro Criptológico Nacional.

- Se tendrán en cuenta los objetivos y la metodología que ofertan para su desarrollo, así como el plan de trabajo.

Las Mejoras a la Oferta técnica. Se valorará:

- Herramientas adicionales aportadas.
- Actuaciones adicionales a realizar en relación al Esquema Nacional de Seguridad.
- Se podrá evaluar también, cualquier otra mejora relacionada con este pliego.

Actividades de formación. Se valorará un mayor número de horas de formación ofertadas.

NOVENA.- Propuesta económica

El presupuesto del contrato es de _____ euros (_____ mil euros), Impuesto del Valor Añadido excluido.

El pago del precio del contrato será realizado al adjudicatario mediante presentación de facturas mensuales por la parte proporcional del importe del contrato y en atención al grado de ejecución del mismo.

DÉCIMA.- Plazo de ejecución

El plazo de ejecución de los trabajos será de _____ (2-7) meses, a contar desde la fecha indicada en el contrato.

UNDÉCIMA.- Documentación de los trabajos

La documentación y/o ficheros generados durante la ejecución del contrato serán propiedad exclusiva de <<LA ENTIDAD LOCAL>>, sin que la empresa adjudicataria pueda conservarlos, ni obtener copia de los mismos o facilitarlos a terceros sin la expresa autorización de la citada organización.
Toda la documentación se entregará en _____ de <<LA ENTIDAD LOCAL>>, en castellano, correctamente encuadernada y con la cantidad de copias que se determinen para cada documento. Asimismo, se entregará dicha documentación en el soporte electrónico que se acuerde para facilitar su tratamiento y reproducción.

DUODÉCIMA.- Protección de datos

<Esta cláusula deberá ser adaptada en la medida en la que el Ayuntamiento tenga implantado el Reglamento Europeo en materia de Protección de Datos, cuyo plazo de adaptación se fija en el mes de Mayo de 2018>

De conformidad con lo Dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa a los interesados de que:

1. Los datos de los licitadores se incorporarán a un fichero de datos personales, denominado _____, del que es responsable <<LA ENTIDAD LOCAL>>, cuya finalidad es la tramitación de los expedientes de contratación sometidos al 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.
2. Cesiones de los datos previstas: a la Junta Consultiva de Contratación; a los restantes candidatos y licitadores; publicaciones en boletines oficiales, tablón de edictos o Web municipal, todo ello de acuerdo con lo previsto en 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, y aquellas otras personas o AA.PP. determinadas por

la legislación especial aplicable al objeto de cada contrato.

3. El órgano administrativo ante el que puede ejercitar, en su caso, los derechos de acceso, rectificación, cancelación, oposición y aquellos otros reconocidos en la normativa vigente en materia de protección de datos de carácter personal, es el Servicio de _____de <<LA ENTIDAD LOCAL>>, situado en _____.

Si el contrato implica el acceso del contratista a ficheros que contengan datos de carácter personal de cuyo tratamiento éste no sea responsable en el sentido del artículo 3.d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el contratista tendrá la consideración de encargado del tratamiento, a los efectos establecidos en dicha Ley Orgánica y su normativa de desarrollo.

El acceso no se considerará comunicación de datos, por ser necesario para la realización de la prestación del objeto del contrato. En todo caso y cuando el contratista tenga acceso a ficheros en los que consten datos de carácter personal de cuyo tratamiento éste no sea responsable, será necesario que en el contrato, o en un documento independiente, se incluyan las cláusulas precisas al objeto de regular dicho acceso, en los términos y con el contenido previstos en la LO 15/1999 y su normativa de desarrollo, sin perjuicio del cumplimiento de los demás requisitos establecidos en la Disposición Adicional 26 del TRLCSP.

Además, el contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá durante un plazo de cinco años desde el conocimiento de esa información, salvo que en el contrato se establezca un plazo mayor.

ANEXO 2.- TABLA DE TAREAS Y RESPONSABILIDADES

En la tabla se usan las siguientes abreviaturas:

CSI – Comité de Seguridad de la Información

RINFO – Responsable de la Información

RSERV – Responsable del Servicio

RSEG – Responsable de la Seguridad

RSIS – Responsable del Sistema

ASS – Administrador de la Seguridad del Sistema

Tarea	Responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba: Dirección
Normativa de seguridad	elabora: RSEG aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

RESPUESTA A INCIDENTES DE SEGURIDAD	
Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.	ASS
Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.	ASS
Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.	ASS
Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.	ASS
Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.	RSEG
Planificar la implantación de las salvaguardas en el sistema.	RSIS
Ejecutar el plan de seguridad aprobado.	RSIS
Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.	Comité de Seguridad de la Información

La tabla siguiente muestra la matriz de Responsabilidades de los distintos actores.

R. - Es responsable de la realización de la tarea señalada.

A. - Es responsable de Aprobar la tarea a realizar, haciéndose responsable de ella una vez aprobada.

C. - Es consultado y se le informa del trabajo hecho.

I. - Es informado sobre el proceso y sus resultados.

Tarea	Dirección	RINF	RSER	RSEG	RSIS	ASS
Niveles de seguridad requeridos por la información		A	I	R	C	
Niveles de seguridad requeridos por el servicio		I	A	R	C	
Determinación de la categoría del sistema		I	I	A/R	I	
Análisis de riesgos		I	I	A/R	C	
Declaración de aplicabilidad		I	I	A/R	C	
Medidas de seguridad adicionales				A/R	C	
Configuración de seguridad		I	I	A	C	R
Aceptación del riesgo residual (1)		A	A	R	I	
Documentación de seguridad (3)				A	C	I
Política de seguridad	A			R	C	I
Normativa de seguridad (3)	A			A	C	I
Procedimientos de seguridad (3)				C	A	I
Implantación de las medidas de seguridad		I	I	C	A	R
Supervisión de las medidas de seguridad				(2)	(2)	R
Estado de seguridad del sistema	I	I	I	A	I	R
Planes de mejora de la seguridad (3)				A	C	
Planes de concienciación y formación (3)				A	C	
Planes de continuidad (3)				C	A	
Suspensión temporal del servicio	A	C	C	C	R	
Seguridad en el ciclo de vida (3)				C	A	

(1) Aparecen dos A porque la aceptación del riesgo residual debe ser coordinada entre ambas responsabilidades. Esta coordinación es muy sencilla si las responsabilidades se aúnan en un Comité de Seguridad de la Información.

(2) Las tareas que realiza el ASS involucran al Responsable del Sistema y al Responsable de la Seguridad. Uno deberá ser el responsable (A) y el otro deberá ser consultado (C). La determinación de quién hace cada papel dependerá de a quién reporta el ASS, pudiendo existir diferentes ASS para diferentes funciones, pero siempre con una línea clara de dependencia de uno u otro responsable.

(3) Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, en cada organismo se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.

EL MODELO DE PLIEGO CONTIENE UNA SERIE DE PAUTAS DE CARÁCTER GENERAL... SE ESPERA QUE CADA ENTIDAD LO PARTICULARICE PARA ADAPTARLO A SU PROBLEMÁTICA CONCRETA

REFERENCIAS

Con objeto de facilitar la forma de acometer los proyectos de adecuación al ENS, ya sea con recursos propios o con terceros, a continuación se relacionan una serie de referencias obtenidas en el momento de redactar esta guía.

Es necesario señalar que la relación de organismos públicos que figuran a continuación es el resultado de una consulta pública y abierta a todos los miembros del Grupo Técnico de la Comisión de Sociedad de la Información y Tecnologías de la FEMP.

Si se desea solicitar ayuda externa para el cumplimiento del ENS, el espectro de empresas es muy amplio y se recomienda consultar en el mercado.

1 Organismos Públicos: Ayuntamientos y Diputaciones

1.1 Ayuntamientos

A.- AYUNTAMIENTO DE MAJADAHONDA

Responsable:

Jaime José López Ruiz

Información General

Hace cuatro años comenzamos a hacer unas auditorías para saber el estado de cara al cumplimiento con el ENS. Acabamos de terminar la segunda.

Plan Administración Electrónica

Comenzamos en su día en el año 2008 con la Región Digital Madrid Noroeste con la implantación de una plataforma de administración electrónica compartiendo recursos tanto económicos como humanos. Primero se incorporamos la factura electrónica, registro electrónico, procedimientos y actualmente estamos progresivamente eliminando el papel a través del expediente electrónico.

Situación Tecnológica

Virtualización de CPD y escritorio parcialmente. Estamos encuadrados

Hoja de Ruta definida para Adecuación al ENS

- Contratación auditoria y Hacking ético
- Inicio auditoria
- Identificación de los servicios
- Calificación de los servicios.
- Detección de deficiencias
- Corrección en lo posible de las deficiencias
- Preparación para la certificación ENS

A destacar

La adecuación al ENS requiere de un esfuerzo tanto de recursos humanos como económicos que no sé cómo se va a poder hacer frente por parte de los Ayuntamientos.

B.- AYUNTAMIENTO DE SANT FELIU DE LLOBREGAT

Responsable:

Mario Alguacil Sanz, Director del Área de Gobierno Abierto y Servicios Generales

Información General

El Ayuntamiento de Sant Feliu de Llobregat aprobó su Plan de adecuación a los esquemas ENS y ENI en diciembre de 2011, cuyo contenido era:

- Política y organización de la seguridad
- Identificación parcial de información, servicios y sistemas (en concreto los de Administración electrónica). La identificación del resto se está haciendo directamente con la herramienta de gestión.
- Los datos de carácter personal (alineando, en este sentido, los requerimientos ENS, ENI y LOPD)
- Las categorías de los sistemas de información
- El análisis de riesgos
- La declaración de aplicabilidad de medidas de seguridad
- Las insuficiencias del sistema
- El Plan de mejora de la seguridad, que preveía 10 proyectos, para alcanzar un Sistema de Gestión de la Seguridad de la Información, entendiendo la seguridad de la información de forma transversal e integral.

El resultado documental y organizativo fue:

- Política de seguridad (alineado con los requerimientos y documentación LOPD)
- Organización de la seguridad en dos órganos colegiados:
  - Comisión de Seguridad, de carácter más institucional. Forman parte concejales delegados y dirección).
  - Subcomisión de Seguridad, de carácter operativo. Forman parte personal técnico del Ayuntamiento.
- Del ENI, el resultado fue:
  - Política de firma electrónica (en revisión actualmente)
  - Política de gestión de documentos (en elaboración)

Plan Administración Electrónica

La estrategia de despliegue de la Administración electrónica en el Ayuntamiento de Sant Feliu de Llobregat tiene como objetivo conseguir una organización administrativa inteligente, estructurada alrededor de una arquitectura integrada de servicios orientada a procesos simplificados y comunes. Se basa en:

- Un modelo de datos único
- La gestión de procesos y documentos:
  - Expedientes electrónicos integrales (cumplimiento nueva normativa de procedimiento), backoffice y frontoffice
  - El sistema de gestión documental integral
- La seguridad de la información como un proceso transversal
- La adecuación a las normas técnicas de interoperabilidad

Situación Tecnológica

El Ayuntamiento de Sant Feliu dispone de 2 CPD's (uno principal y secundario) con una red de comunicaciones propias (fibra óptica) y segura que los enlaza con los diferentes edificios municipales.
Las aplicaciones corporativas se basan en software de mercado, en desarrollos a partir de soluciones estándar y en servicios de terceros (principalmente de la Administració Oberta de Catalunya).

Hoja de Ruta definida para Adecuación al ENS

» Aprobación de la Política de Seguridad
» Elaborar un plan de adecuación para la mejora de la seguridad
» Realizar el análisis de riesgos que incluya la valoración de las medidas de seguridad existentes
» Preparar y aprobar la Declaración de aplicabilidad
» Implantar, operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad
» Auditorías
» Informar sobre el estado de la seguridad

Otras certificaciones

No se disponen de certificaciones de gestión de seguridad de la información.

A destacar

El Ayuntamiento de Sant Feliu desarrolla diversas soluciones que comparte con otros Ayuntamientos y Administraciones Públicas. Estas soluciones responden a problemáticas concretas sin que tengan un nivel de servicio o criticidad significativa en los servicios al ciudadano: Smart Cities, etc.

C.- AYUNTAMIENTO DE PALENCIA

Responsable:

José Luis Pons Martín

Información General

Actualmente el Ayuntamiento de Palencia se encuentra en pleno desarrollo de implementación del ENS, proyecto de ayudas con fondos europeos EDUSI y el proyecto DIGIPAL a través de Red.es con el objetivo de convertir la ciudad de Palencia en un territorio más inteligente, promoviendo el desarrollo de un conjunto coordinado de actuaciones, mediante el uso de las TIC.

Plan Administración Electrónica

El Plan de acción sobre administración electrónica identifica dos prioridades políticas:

- La modernización de las administraciones públicas utilizando identificación electrónica, firma electrónica. En pleno proceso de implementación.
- Facilitar la interacción digital entre las administraciones y los ciudadanos/empresas de servicios públicos de calidad. Adecuación a través del proyecto DIGIPAL y EDUSI actualmente en proceso de desarrollo.

Situación Tecnológica

El Ayuntamiento de Palencia dispone de un CPD principal situado en la casa consistorial y otro que se utiliza principalmente para backup y réplica de algunos servicios en las instalaciones de la Policía Municipal. Prácticamente todas las instalaciones del Ayuntamiento se conectan al CPD principal, utilizando VPN y por medio de fibra. Los servicios que ofrece el Ayuntamiento se encuentran alojado en el CPD, salvo la página web y la intranet municipal que se encuentran alojadas en un proveedor hosting.

Hoja de Ruta definida para Adecuación al ENS

El proceso de adecuación al ENS se ha organizado en dos grandes grupos de tareas que pueden ir realizándose de forma paralela:

1. **Actualización del borrador del Plan de Adecuación al ENS actual, al nuevo alcance,** conforme a lo establecido en la Guía CCN-STIC-830 Ámbito de aplicación del ENS, que consiste en:
    - Asignación de roles de seguridad establecidos por la normativa ENS, y constitución del comité de seguridad de la Información. Tareas que actualmente se encuentran pendientes de aprobación.
    - Actualizar el inventario de servicios e información y proceder a su valoración, aunque sea de manera informal, en caso de que no se haya nombrado a los responsables de los servicios y la información (inicialmente se prevé que el nivel máximo alcanzado para la categoría de los sistemas sea nivel MEDIA).
    - Actualización del análisis de riesgos.
    - Actualización de la declaración de aplicabilidad.
    - Actualización del informe de suficiencias del sistema.
    - Actualización del Plan de mejora de la seguridad.
    - Aprobación del Plan de Adecuación

2. **Implantación de medidas de seguridad del anexo II del Real Decreto ENS**
    - » Proceder a la implantación de las medidas de seguridad del anexo II del Real Decreto EN, que se encuentran recogidas en el Plan de Mejora de la Seguridad.
    - » Actualización y control de ejecución de las medidas de seguridad recogidas en el Plan de mejora de la seguridad.

Otras certificaciones

No se dispone de certificaciones.

A destacar

La implementación del ENS en el Ayuntamiento de Palencia supone un constante cambio de los medios tecnológicos para cumplir con las actualizaciones de normativa y avances técnicos, para ello es importante la ayuda que se pueda prestar tanto para la renovación de componentes Hardware y Software como del soporte a través de recursos humanos especializados en la materia.

El Ayuntamiento realiza de forma periódica auditorías de cumplimento en materia de protección de datos, ENS, y transparencia.

D.- AYUNTAMIENTO DE PICANYA

Responsable:

Fernando Gallego García

Información General

Municipio de 11.500 habitantes que comenzó proyectos de administración electrónica en el año 2008. Actualmente cuenta con prácticamente el 100% del procedimiento electrónico y todo él mediante procesos a medida en BPM.

Plan Administración Electrónica

Actualmente estamos potenciando la parte frontal, el desarrollo de plantillas y formularios para todos los trámites en sede electrónica, y la implantación de un portal tributario más completo que el que tenemos. Acabamos de aprobar ordenanza de administración electrónica y política de gestión de documento y expediente electrónicos. El futuro inmediato pasa por terminar de integrar con las herramientas del estado. Actualmente en uso @firma, y en desarrollo SIR y Notific@. A la espera de Archiv-e.

Situación Tecnológica

La infraestructura está alojada íntegramente en el ayuntamiento, con muy pocos o ningún servicio externalizado. Trabajamos con hosts virtualizados y entornos de pre y post producción. Todos los centros están conectados por fibra, y los agentes externos (empresas colaboradoras, algunos concejales) entran a las aplicaciones vía Web o Mobile. Nuestro reto más inmediato es la mejora y adecuación del sistema de red mediante particionado en VLAN y el cambio del sistema de seguridad perimetral que tenemos obsoleto, todo esto alineado con ENS.

Hoja de Ruta definida para Adecuación al ENS

a. Planificación implantación ENS y adecuación a Reglamento Europeo de Protección de Datos
b. Adecuación de red / seguridad perimetral / sistemas de impresión
c. Diagnóstico
d. Aprobación de plan de implantación ENS
e. Desarrollo

Otras certificaciones

Hemos estado certificados en ISO 9002 y Carta de Servicios, pero desde el año 2016 ya no se pasan auditorías con lo que se nos retiran las certificaciones. Internamente seguirnos trabajando según sistema de compromisos

E.- AYUNTAMIENTO DE CARTAGENA

Responsable:

José López Martínez

Información General

El Ayuntamiento de Cartagena no se encuentra adecuado al ENS, aunque está adoptando medidas para conseguir la adecuación al mismo. Mientras, se están aprobando normas y se dispone de procedimientos propios de seguridad que ofrecen garantía suficiente.

Plan Administración Electrónica

El Ayuntamiento ha identificado como ejes esenciales para la adecuación a la legislación en la materia un plan de formación, un análisis y simplificación de procedimientos, un desarrollo normativo y un desarrollo tecnológico. Puesto que es un proyecto ambicioso que escapa a los recursos propios del Ayuntamiento, se están contratando los servicios de desarrollo tecnológico y, siempre que es posible, de simplificación administrativa.

Situación Tecnológica

El Ayuntamiento dispone de su propio Centro de Proceso de Datos, aunque algunos servicios se encuentran alojados en Cloud. Los lenguajes de programación más habituales son ASP, .NET, javascript y,

ocasionalmente, PHP. Se adoptan medidas de seguridad como firewalls, antivirus, copias de seguridad, proxy, etc., pero no se hace aún de manera normalizada y regulada.

Hoja de Ruta definida para Adecuación al ENS

a. Política de seguridad en vigor
b. Normativa de seguridad en vigor
c. Procedimientos en proceso de elaboración
d. Permisos, existentes pero no regulados
e. Adecuación y certificación en el ENS pendiente de contratación con empresa externa

Se espera contar con tal certificación en el primer semestre de 2018

Otras certificaciones

No se cuenta con certificaciones de seguridad, salvo en aplicaciones externas, como la de Archivo.

1.2 Diputaciones Provinciales, Consejos y Cabildos Insulares

A.- DIPUTACIÓ PROVINCIAL DE CASTELLÓ

Responsable:

Borja Colón de Carvajal Fibla

Información General

La Diputación de Castellón está llevando a cabo actualmente una auditoría en materia de ENS que pretende concluir, además de con una actualización de su actual Plan de Seguridad, con un documento de conformidad al ENS.

Plan Administración Electrónica

Nuestro plan de Administración electrónica si incluye dentro de la estrategia de innovación y creación de valor público como eje principal para la consecución de una administración más eficiente y sostenible.

Situación Tecnológica

Contamos con un potente gestor de expedientes, sede electrónica en pleno funcionamiento, política de firma, modelo de gestión de documentos electrónicos, portal de transparencia y open data.

Hoja de Ruta definida para Adecuación al ENS

La Diputación de Castellón dispone del Plan de Adecuación al ENS, en el que ha acometido las siguientes tareas:

a. Definición de Política de Seguridad
b. Definición de estructura de roles y responsabilidades
c. Inventario de información manejada, junto con su valoración
d. Inventario de servicios que se prestan, junto con su valoración
e. Inventario de sistemas de información, junto con su categorización
f. Realización de un análisis de riesgos formal, con metodología Magerit v.3

g. Realización de declaración de aplicabilidad, con respecto al ENS, LOPD y RGPDUE
h. Análisis de Insuficiencias del sistema con respecto a las 75 medidas recogidas en el Anexo II del ENS
i. Realización del plan de mejora de la seguridad

En la actualidad, la Diputación de Castellón va a implantar medidas técnicas y organizativas, de acuerdo con el plan de mejora de la seguridad.

Antes de final de año, se acometerá la auditoria de conformidad y se acometerán las medidas correctivas y preventivas resultantes de la misma, a fin de continuar con el plan de mejora continua.

Otras certificaciones

No dispone.

A destacar

Fuimos la primera institución pública española en superar una auditoría externa en transparencia y buen gobierno.

Se ha considerado que dados los esfuerzos tanto humanos como organizativos necesarios para lograr el pleno cumplimiento del ENS, acometer en el mismo plazo de tiempo, el plan de adecuación al Esquema Nacional de Interoperabilidad, así como la actualización de las medidas requeridas por la LOPD y RGPDUE. De esta forma, se integran los cuatro marcos normativos, dando como resultado, una visión completa de la seguridad desde las diferentes perspectivas.

B.- DIPUTACIÓN PROVINCIAL DE PALENCIA

Responsable:

Beatriz Bahillo Sáez

Información General

Disponemos de un Comité de seguridad y designación de responsables y los preceptivos protocolos de la política de seguridad aprobada por el Pleno Corporativo (BOP 18 de junio 2014).

Plan Administración Electrónica

Disponemos de un Plan de Innovación aprobado por la Junta de Gobierno en octubre del año 2015 y estamos en elaboración de un Plan de implantación de Administración Electrónica.

Situación Tecnológica

Positiva.

Hoja de Ruta definida para Adecuación al ENS

MEDIDAS PRIORIZADAS	EJECUCIÓN
Constitución del Comité de Seguridad y asignación de Responsabilidades ENS	Sí
Aprobación y publicidad de la Política de Seguridad de la Información	Sí
Auditorías ENS (periodicidad bienal)	Sí
Actualización del Análisis de Riesgos (periodicidad anual)	2017
Aprobación de toda la gestión documental asociada a la Elaboración del Plan de Adecuación al ENS por el Comité de Seguridad	Sí
Aprobación y publicación del Plan de Adecuación al ENS	Pendiente
Definición y elaboración de la normativa de seguridad. Políticas de uso correcto sistemas información, uso internet y correo electrónico,.. etc.	Sí
Aprobación, publicación, difusión e implementación de la normativa de seguridad	Sí
Documentar la Seguridad de la Información. Realización del esqueleto del SGSI	Pendiente
Implementación de mecanismos de difusión (al personal involucrado) de los procedimientos de seguridad.	Sí
Auditoría LOPD Diputación (periodicidad bienal)	Sí
Regulación de los Servicios Externos	Pendiente
Gestión de la seguridad en los Recursos Humanos	Pendiente
Revisión y/o adaptación de medidas que garantizan un correcto acceso al sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Revisión y/o adaptación de las necesidades operacionales del sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Revisión y/o adaptación de medidas que garantizan el correcto funcionamiento del sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Revisión y/o adaptación de medidas que garantizan la protección del sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Seguridad de la Sede. Test de penetración	Pendiente

Otras certificaciones

Ninguna.

A destacar

Realización de auditorías periódicas y participación en la Encuesta Nacional del Estado de la Seguridad (INES el 20-01-2017).

C.- DIPUTACIÓ PROVINCIAL DE LLEIDA

Responsable:

Gerard Serra/ Ramón Siuraneta

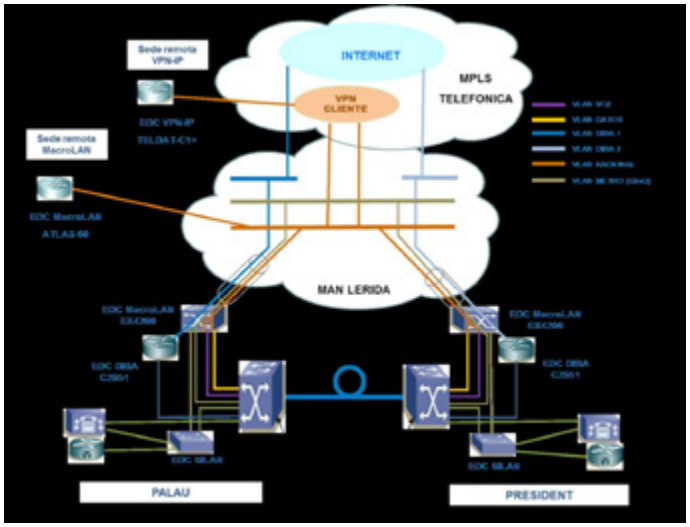
Información General

En el año, a través de una consultora externa se procedió a revisar, adecuar información, datos, servicios, aplicaciones, equipos y todos los recursos de servicios a ciudadanos.

Plan Administración Electrónica

La Diputación de Lleida dispone de una hoja de ruta de implantación de la e-administración período 2016/2019 en los ámbitos normativo, de gestión documental, organizativo y tecnológico con indicadores de cumplimiento de la leyes 39/2015 i 40/2015.

Situación Tecnológica



Hoja de Ruta definida para Adecuación al ENS

Fase Inicial Abril/diciembre 2015:

- Fase 1.- Planificación inicial y lanzamiento.
- Fase 2.- Análisis situación actual.
- Fase 3.-Evaluación riesgos y controles
- Fase 4.- Emisión de resultados

Fase definición Plan de adecuación Enero/marzo 2016:

» Definición del Plan de Adecuación al ENS de la Diputación y todos sus organismos.

Fase Elaboración Marco Normativo, Marzo/abril 2016:

» Fase1.- Identificación y análisis de requisitos

» Fase 2: Desarrollo y aprobación marco normativo

» Fase 3: Revisión y desarrollo procedimientos operativos de seguridad

Se espera contar con tal certificación en el primer semestre de 2018

Otras certificaciones

No tenemos.

A destacar

Para este año tenemos previsto tener toda la adecuación terminada.

D.- DIPUTACIÓ PROVINCIAL DE VALENCIA

Responsable:

Eusebio Moya López

Información General

Se dispone de toda la estructura organizativa de seguridad (Comité de seguridad, Responsable de Seguridad y resto de responsables); así como Reglamento de Política de Seguridad (acuerdo del Pleno de la Corporación 18 de junio de 2013, BOP 159, de 6 de julio) y normativa interna de desarrollo.

Plan Administración Electrónica

Existe un Reglamento de desarrollo de Administración Electrónica de la Diputación de Valencia (acuerdo del Pleno de 21 de mayo de 2013, BOP 232, de 30 de septiembre), así como un Reglamento de Política de Gestión de Documentos Electrónicos (acuerdo del Pleno de 17 de junio de 2014, BOP 297 de 15 de diciembre de 2014).

Situación Tecnológica

El entorno tecnológico de los sistemas de información es favorable para la implementación del ENS.

Hoja de Ruta definida para Adecuación al ENS

	ACCIONES PROYECTADAS	NIVEL DE EJECUCIÓN
1	Aprobación Política de Seguridad	Cumplimentado
2	Constitución Comité STIC	Cumplimentado
3	Desarrollo normativas internas	Cumplimentado
4	Desarrollo procedimientos internos	Intermedio
5	Formación personal	Intermedio
6	Exigencia requisitos ENS a terceros	Cumplimentado
7	Inventario activos y análisis de riesgos	Cumplimentado
8	Auditorías periódicas externas	Cumplimentado
9	Implementación medidas de seguridad marco operacional y medidas de protección	Proceso continuo
10	Implantación SGSI	Incipiente

Otras certificaciones

La Corporación se encuentra actualmente en un proceso para obtener la Certificación de Conformidad con el ENS, de sistemas de categorías MEDIA o ALTA, conforme a lo establecido en la Instrucción Técnica de Seguridad de Conformidad con el ENS(Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas)

A destacar

La Corporación mantiene líneas para facilitar que, tanto sus organismos públicos vinculados o dependientes, como las Entidades Locales de su territorio, cumplan las previsiones del ENS

E.- DIPUTACIÓN PROVINCIAL DE SEVILLA

Responsable:

Carmen Rodríguez Quirós, Gerente Sociedad Informática (INPRO).Diputación de Sevilla

Información General

La Diputación de Sevilla centraliza toda la gestión a través de INPRO, Sociedad Informática instrumental de la misma, para la prestación de Servicios Informáticos a la propia Diputación y a los Ayuntamientos de la Provincia, INPRO tiene como objeto poner en marcha las políticas del equipo de gobierno en materia de modernización, innovación e implantación de las TICs y la informatización de los Servicios de la Diputación en beneficio de los Ayuntamientos, y de la propia gestión de Ayuntamientos y Entidades Locales de la Provincia.

Plan Administración Electrónica

Desde el año 2011 INPRO ha desplegado una Plan estratégico para el desarrollo e implantación de la Administración Electrónica. Actualmente son 79 Ayuntamientos con Sede Electrónica Publicada. Un proyecto en marcha de Intercambio Registral en toda la Provincia, plataformas desplegadas de forma generalizada de firma electrónica, resoluciones, videoactas, convocatorias telemáticas, etc. A ello se suma la plataforma de Tramitación Electrónica MOAD-H desarrollada a través del convenio con la Junta de Andalucía de la que se benefician 5 diputaciones Andaluzas.

Situación Tecnológica

Todos los servicios se ofrecen a través de una Red Provincial, actualmente en proceso de renovación, RED TARSIS, donde se da servicio de forma centralizada desde el CPD de la Diputación de Sevilla a todos los Ayuntamientos. Los Ayuntamientos conectados acceden a través del Portal Provincial a todas las herramientas corporativas, y se incluye asistencia técnica y acompañamiento tecnológico por parte de INPRO.

Hoja de Ruta definida para Adecuación al ENS

La Diputación de Sevilla tras encomienda a INPRO, se ha estado trabajando desde Septiembre de 2016 en las siguientes fases:

- Revisión de todos los aspectos de seguridad organizativa y legal (Documentos de seguridad, roles y Identificación y valoración de activos en el alcance del ENS y estudiar y valorar las medidas de seguridad de operación y explotación de sistemas y comunicaciones - Estudio de medidas de seguridad sobre el diseño de aplicaciones y base de datos (acceso lógico, logs, protección de datos) y metodologías de desarrollo.
- Medidas de protección de los puestos de usuario
- Medidas de seguridad física en oficinas y puestos de usuario
- Valorar contratos con empleados y plan de formación, en lo que respecta al ENS
- Estudiar los contratos con terceros

A partir de este estudio se ha tenido en Enero de 2017 los siguientes resultados:

» Cuestionario INES cumplimentado
» Plan de adecuación al ENS
» Política de seguridad
» Relación de medidas a adoptar

Actualmente nos encontramos en el trámite administrativo de aprobación en Pleno, información a Directores y posterior adopción de medidas. Las medidas adoptadas tienen un cronograma para cada una, llegando a la finalización total con previsión marzo de 2018.

Una vez finalizado el nuestro, dado que los Ayuntamientos menores de 20.000 habitantes en un 90% tienen sus servicios informáticos residentes en la Diputación de Sevilla, queremos establecer un Plan de Adecuación ENS tipo que con apoyo de una consultora especializada e INPRO pueda finalizar en un plan de adecuación ENS propio para cada uno de los Ayuntamientos que se adhieran a este plan. (Previsión para 2018).

A destacar

La Diputación de Sevilla a través de INPRO tiene asumida la gestión centralizada de la Administración Electrónica, definición tecnológica de la red de cada Ayuntamiento, su incorporación a la Red Provincial TARSIS, la formación a sus empleados y el asesoramiento continuo junto con el despliegue de todas las Aplicaciones informáticas necesarias para el cumplimiento de las obligaciones digitales de la Ley 39 y 40 del año 2015.

F.- CABILDO INSULAR DE GRAN CANARIA

Responsable:

Ana María Colás Rocha

Información General

Se ha estado trabajando en relación a la adecuación al ENS en los últimos dos años. Al inicio fue necesaria ayuda externa y posteriormente se asumió la continuidad internamente.

Plan Administración Electrónica

El plan de puesta en marcha de la Administración Electrónica está en fase de elaboración por lo que los trabajos actualmente en ejecución se centran en la ampliación del número de procedimientos existentes en la Sede Electrónica y la incorporación de herramientas de backoffice que permitan la gestión de expedientes electrónicos. Los circuitos de tramitación contable son electrónicos. El sistema de contratación electrónica se encuentra al 50% de implantación. Volumen de firmas electrónicas actual: 250.000 anuales.

Situación Tecnológica

La implantación tecnológica de herramientas de administración electrónica evoluciona favorablemente aunque sería necesario acelerarla para cumplir las Leyes 39 y 40. Se presta servicio centralizado a Organismos Autónomos y otros entes dependientes y se desea ampliar el servicio a los municipios. Los RRHH dedicados a las TICs son escasos.

Hoja de Ruta definida para Adecuación al ENS

Existe un borrador de política de seguridad y de algunas normativas, procedimientos, etc. Dichos documentos podrán tener que ser modificados en función del texto definitivo que tenga la Política de Seguridad.

1. Aprobación de la Política de Seguridad
2. Revisión de las siguientes Normativas, Procedimientos y Herramientas (en base a los posibles cambios derivados de la aprobación definitiva de la política) Nota: se aplican "de facto":
    - Normativa General de utilización de los Recursos y Sistemas de Información
    - Normativa de Creación y Uso de Contraseñas
    - Normativa de Acceso a Internet
    - Normativa de Uso de Correo Electrónico
    - Normativa de desarrollo software
    - Normativa de Control de Acceso Lógico
    - Normativa de Generación de Copias de Respaldo y Recuperación de la Información
    - Procedimiento de gestión de solicitudes de copias de respaldo y recuperación de la información
    - Procedimiento de Gestión de Usuarios: altas, bajas recursos
    - Procedimiento de Clasificación y Tratamiento de la Información
    - Procedimiento de Registro y Gestión de Incidencias
    - Procedimiento de Gestión de Soportes
    - Procedimiento de promoción de un proyecto entre capas
    - Procedimiento de aceptación de un proyecto
    - Procedimiento de entrada y salida de personas y equipos del CPD
    - Procedimiento de limpieza de metadatos
    - Áreas separadas y con control de acceso
    - Herramienta gestión de claves

3. Instrucción técnica sobre la seguridad en ordenadores personales
4. Registro de aceptación y compromiso cumplimiento Normativa General de utilización de los Recursos y Sistemas de Información
5. Continuar con la elaboración de los siguientes documentos y herramientas (se aplica "de facto" pero falta documentar):

» Plan de formación en seguridad TIC
» Plan de concienciación en seguridad TIC
» Procedimiento de análisis de riesgos
» Procedimiento de adquisición de nuevos componentes
» Procedimiento de gestión del inventario de activos
» Procedimiento de gestión de la configuración
» Procedimiento de gestión de cambios
» Procedimiento de protección frente a código dañino
» Procedimiento de gestión de claves criptográficas
» Procedimiento de gestión de suministradores
» Procedimiento de protección de las instalaciones
» Procedimiento de gestión de las comunicaciones
» Procedimiento de auditoria del ENS
» Procedimiento de protección de los servicios
» Procedimiento de supervisión y monitorización del sistema
» Formación
» Concienciación
» Gestión de la capacidad
» Configuración de seguridad
» Mecanismo de autenticación
» Criptografía
» Clasificación de la Información
» Gestión de incidencias
» Documento arquitectura de seguridad
» Documento de roles y responsabilidades

Otras certificaciones

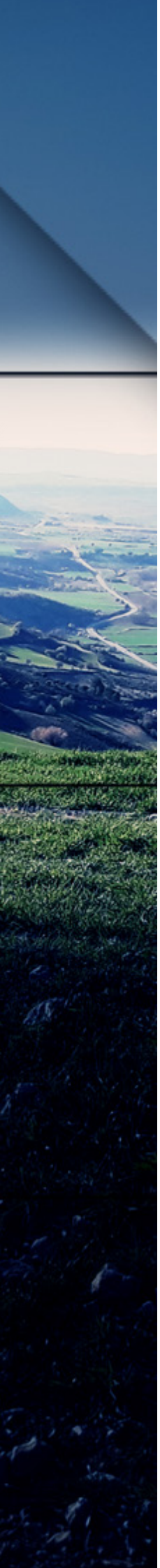
Mientras no se realice la aprobación de la Política de Seguridad no es posible realizar certificaciones.

A destacar

Complejidad de hacer entender a los cargos electos la necesidad de tener aprobada y aplicar una Política de Seguridad.


FEMP
FEDERACION ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS

GLOSARIO Y DEFINICIONES DE TÉRMINOS



A fin de conocer la seguridad que ofrece un sistema, necesitamos modelarlo, identificando y valorando los elementos que lo componen y las amenazas a las que están expuestos. Con estos datos podemos estimar los riesgos a los que el sistema está expuesto.

ENS

Esquema Nacional de Seguridad

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. ENS.

ACREDITACIÓN

Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información de un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.

ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)

Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad. OM 76/2002.

> (en) *Information System Security Officer. Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. CNSS Inst. 4009, Adapted*

ALCANCE DE LA AUDITORÍA

Elementos a los que comprende la revisión de auditoría: los sistemas que estarán en revisión, el organismo responsable de estos sistemas, los elementos de la estructura tecnológica, personal vinculado a los elementos anteriores, periodos de tiempo. Dentro del contexto de esta guía tiene una relación directa con la Declaración de Aplicabilidad.

AMENAZA

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

AMENAZA PERSISTENTE AVANZADA (APT)/*AdvancedPersistentThreat (APT)*

Un ataque selectivo de ciberespionaje o cibersabotaje, llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados es una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. McAfee. Predicciones de amenazas para 2011.

ANÁLISIS O VALORACIÓN DE RIESGOS

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. ENS.

Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema (STIC 811)

AUDITOR

El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. Realiza las tareas de auditoría.

CRITERIOS DE RIESGO

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. [UNE Guía 73:2010]

AUDITOR INTERNO

Pertenece a una unidad independiente dentro del organismo al que pertenecen los elementos objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión de los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad debe reportar al nivel jerárquico más alto dentro del organismo.

AUDITOR EXTERNO

Es independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar.

AUDITORÍA

Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

- Nota 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).
- Nota 2: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011. [ISO, Anexo SL]

AUDITORÍA DE LA SEGURIDAD

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. ENS

Equipo de trabajo

COORDINACIÓN:

Virginia Moreno (Ayuntamiento de Leganés)

ELABORACIÓN GUÍA/CUADERNO DE TRABAJO/REDACCIÓN:

Carlos Galán (UC3M – ATL).
Javier Candau (CCN).
Javier de la Villa (Diputación de León).
Javier Peña y Jorge Pérez (Diputación de Burgos).
Miguel Ángel Amutio (MINHAFP).
Miguel Ángel Lubián (CIES).
Virginia Moreno (Ayuntamiento de Leganés)

COORDINADOR FEMP

Pablo Bárcenas (Secretario Comisión de SSII y TT)

AGRADECIMIENTOS:

Ayuntamiento de Cartagena
Ayuntamiento de Majadahonda
Ayuntamiento de Palencia
Ayuntamiento de Picanya
Ayuntamiento de Sant Feliu de Llobregat

Diputación de Castellón
Cabildo de Gran Canaria
Diputación de Lleida
Diputación de Palencia
Diputación de Sevilla
Diputación de Valencia
Diputación de León
Diputación de Burgos

Agencia de Tecnología Legal

Instituto CIES

Grupo de Trabajo de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

Calle Nuncio 8 28005,
Madrid. España

femp@femp.es

www.femp.es