CCN-CERT
centro criptológico nacional

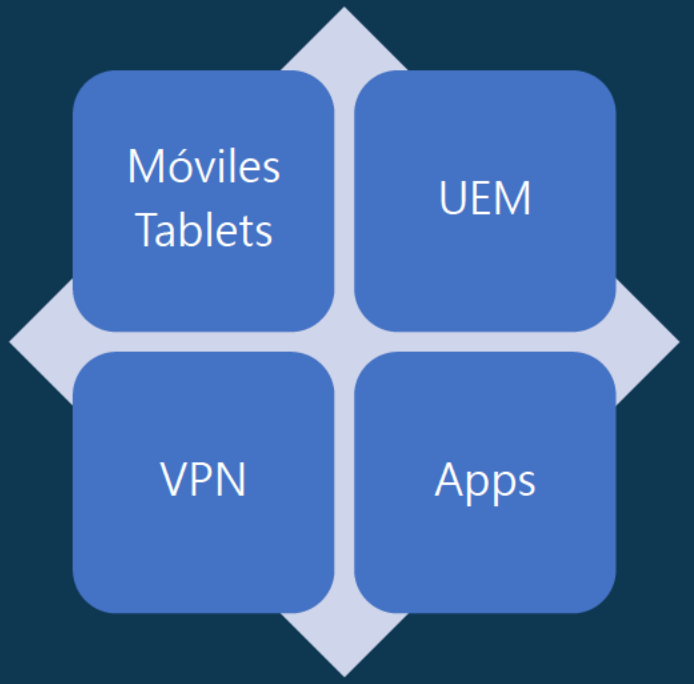
LA SEGURIDAD EN LOS DISPOSITIVOS MÓVILES

(diciembre 2020)

CCN-CERT
centro criptológico nacional

La seguridad en los dispositivos móviles
¿Por qué hemos realizado esta convocatoria?

- ☆ Dar a conocer la arquitectura de comunicaciones móviles propuesta por el CCN,
- ☆ Presentar soluciones que permitan aumentar la ciberseguridad de los sistemas de comunicaciones móviles,
- ☆ Resolver dudas



La seguridad en los dispositivos móviles
La necesidad

☆ Desde un punto de vista funcional, se ha expandido el concepto de las *Everywhere Enterprises* (empresas en las que se trabaja desde cualquier lugar), pasando en muchas organizaciones al Remote First (Teletrabajo prioritario).

Organismos y empresas permiten a sus empleados trabajar desde cualquier lugar, incrementado con ello el uso de los dispositivos móviles (y abriendo nuevas puertas de acceso a los cibercriminales).

☆ Las guías y recomendaciones elaboradas por el CCN (Centro Criptológico Nacional), nos ayudan a aumentar la seguridad de los sistemas TIC de la Administración y su adaptación al Esquema Nacional de Seguridad (ENS). Facilitan además al obligado cumplimiento de las normativas europeas y estatales tales como RGPD.

La seguridad en los dispositivos móviles
Una reflexión

Algunas preguntas que debiéramos hacernos antes de continuar:

☆ ¿Estás sujeto a las regulaciones que requieren protección de datos?
☆ ¿Son tus protecciones suficientemente completas?
☆ ¿Tienen los usuarios acceso a datos críticos / sensibles desde sus dispositivos móviles?
☆ ¿Qué porcentaje de tus datos es accesible desde dispositivos móviles?
☆ ¿Cómo estás asegurando los dispositivos y los datos?
☆ ¿Das a los dispositivos móviles la consideración de *End Point*?
☆ ¿Tienes una detección de amenazas y una estrategia de defensa?

¿Estás protegiendo a los dispositivos móviles como al resto de tu infraestructura?

En caso contrario, ¿Por qué has elegido dejar expuestos los dispositivos móviles?

La seguridad en los dispositivos móviles
Las amenazas

☆ Las amenazas más peligrosas para los dispositivos móviles en la actualidad son:

- ☆ *TROYANOS MÓVILES DE ACCESO REMOTO (mRATs) (1)*
- ☆ *ATAQUES WiFi MAN-IN-THE-MIDLE (MitM) (2)*
- ☆ *ATAQUES DE DÍA ZERO (3)*
- ☆ *EXPLOTACIÓN DE PRIVILEGIOS (4)*
- ☆ *CERTIFICADOS FALSOS (5)*
- ☆ *PERFILES MALICIOSOS (6)*
- ☆ *VULNERABILIDAD EN WEBKIT (7)*
- ☆UN USUARIO DESINFORMADO

☆FALTA DE UNA POLITICA DE SEGURIDAD CORPORATTIVA QUE TENGA EN CUENTA LOS PROBLEMAS ESPECIFICOS DE LOS DISPOSITIVOS MÓVILES

Sobre estos SI podemos actuar

(1) Dan la capacidad de obtener de forma remota el acceso a todo lo almacenado, pudiendo infectar tanto sistemas Android como iOS. En dispositivos Android se infectan a través de aplicaciones del 'Marketplace' de Google y los iOS son igualmente vulnerables a través del método 'Jailbreak'.
(2) Ocurren cuando un dispositivo se conecta a un punto de acceso WiFi que ha sido infectado. El atacante se hace con las comunicaciones y puede escuchar de forma secreta e incluso alterar la comunicación de la red.
(3) Suponen la explotación de ciertas vulnerabilidades, tanto en iOS como Android, que aun no han sido publicadas. Una vez en el dispositivo, el atacante puede robar contraseñas, datos corporativos y correos electrónicos, así como recoger información de actividad del teclado y pantalla.
(4) Las vulnerabilidades de Android pueden ser explotadas para obtener altos privilegios sin dejar rastro, como sucedió con la vulnerabilidad 'Certi-gate' que afectó a cientos de millones de dispositivos el pasado verano. Los ataques se aprovechan de las oportunidades creadas por la fragmentación de Android.
(5) Usan certificados de distribución para hacer 'Slideloading' de una aplicación, dejando a un lado el proceso de validación oficial de la tienda de aplicaciones Apple mediante una descarga directa en el dispositivo.
(6) Utilizan los permisos de perfil para eludir los mecanismos de seguridad típicos, permitiendo, por ejemplo que el atacante modifique el recorrido del tráfico de un usuario desde el dispositivo móvil a un servidor controlado por él.
(7) Permiten a los navegadores web renderizar las páginas de forma correcta para un usuario. Los ciberdelincuentes las explotan para ejecutar 'scripts' propios, dejando a un lado las robustas medidas de seguridad implementadas por Apple

Los dispositivos móviles corporativos y el acceso a información corporativa desde otros dispositivos móviles exigen un tratamiento diferenciado de otro tipo de equipos, tales como ordenadores de sobremesa o portátiles.

La seguridad en los dispositivos móviles
BYOD, Shadow IT y riesgos derivados

- ☆ En el caso de los dispositivos móviles encontramos muchas veces dispositivos que son propiedad de los usuarios (BYOD), o dispositivos que siendo propiedad de la organización, son utilizados en el ámbito personal (COPE). Esto puede generar importantes inconvenientes en materia de seguridad tanto de su configuración como de un uso inseguro.
- ☆ Es necesario crear y mantener configuraciones de seguridad diferentes para cada perfil de usuario y dispositivo, para mitigar los riesgos de manera proporcional en cada caso.

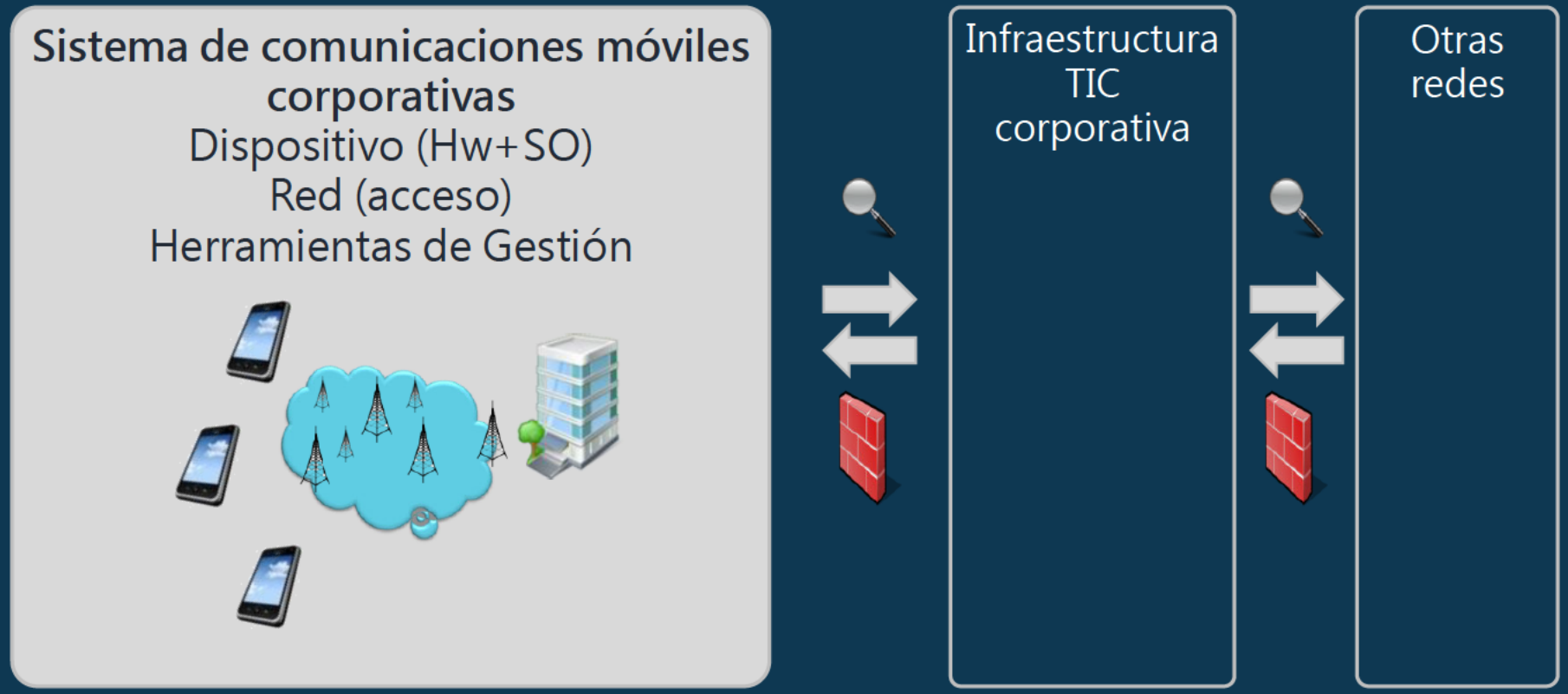
	Dispositivo corporativo	**Otros dispositivos**
Dirección	Configuración 1A	Configuración 1B
Empleado interno	Configuración 2A	Configuración 2B
Empleado externo	Configuración 3A	Configuración 3B
Desatendidos	Configuración 4A	N/A

☆Objetivos de seguridad para los sistemas de comunicaciones móviles :

- ☆ ***Confidencialidad e Integridad:*** Garantizando que la información enviada, recibida o almacenada por el dispositivo no puede ser leída por terceros no autorizados.
- ☆ ***Disponibilidad:*** Garantizando que los recursos que necesitan los usuarios (del propio dispositivo o externos a él), están disponibles siempre que se necesitan.
- ☆ ***Autenticación:*** garantizando que el dispositivo móvil no está siendo suplantado por otro.
- ☆ ***Trazabilidad:*** Garantizando el seguimiento y la determinación de los tratamientos efectuados en el dispositivo.

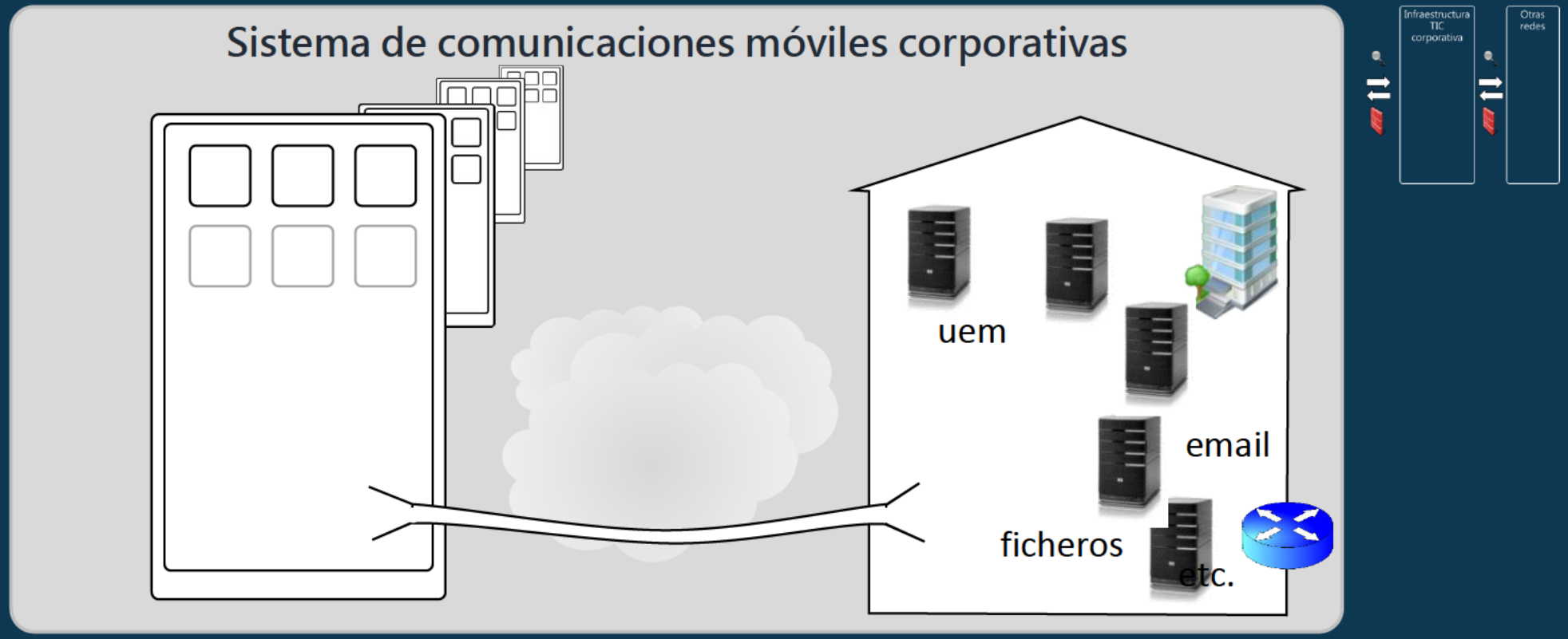
La seguridad en los sistemas de comunicaciones móviles
Arquitectura de seguridad

☆ La arquitectura del sistema se diseña para poder gestionar los riesgos :



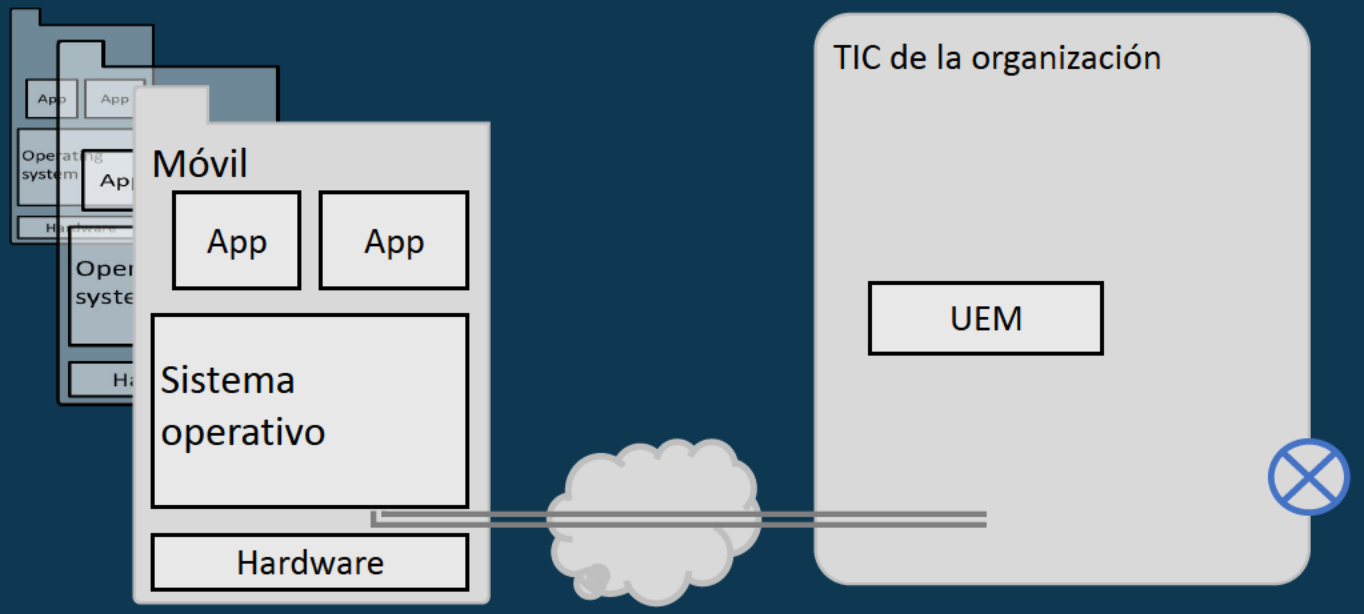
La seguridad en los sistemas de comunicaciones móviles
Arquitectura de seguridad

☆ La arquitectura del sistema se diseña para poder gestionar los riesgos :



La seguridad en los sistemas de comunicaciones móviles
Arquitectura de seguridad

☆ El CCN estructura los productos que considera aptos para su despliegue en familias y categorías dentro del Catalogo de Productos de Seguridad de las TIC:



Familia CPSTIC

- ☆ Dispositivos Móviles
- ☆ Redes Privadas Virtuales
- ☆ Herramientas de Comunicaciones móviles seguras
- ☆ Herramientas de Gestión de dispositivos móviles UEM /MDM

La seguridad en los sistemas de comunicaciones móviles

Productos necesarios para el despliegue

☆ El Catálogo de Productos de Seguridad de las TIC (CPSTIC) es el listado en el que el CCN estructura los productos que han superado un proceso de cualificación:

☆ Incluye aquellos productos y servicios que forman parte de la arquitectura de seguridad de un sistema de información.

☆ Permite a los organismos de la Administración simplificar el proceso de selección y despliegue de productos TIC

☆ Productos organizados por familias según su funcionalidad.

☆ Para cada familia se definen unos RFS (Requisitos Fundamentales de seguridad)

☆ Los productos y servicios incluidos en el CPSTIC disponen de una certificación funcional de seguridad conforme a los RFS de su categoría/familia.

CCN-PYTEC
centro criptológico nacional

La seguridad en los sistemas de comunicaciones móviles
Resumen

- ☆ El impulso de la movilidad y los escenarios de teletrabajo hace que sea necesario implementar estrategias de ciberseguridad adaptadas a los nuevos escenarios y retos.
- ☆ Es fundamental proteger los dispositivos móviles (end point móviles) que tienen acceso a nuestros sistemas.
- ☆ El despliegue de dispositivos en modo COBO permite garantizar el cumplimiento de regulaciones y normativas sobre la protección del dato y de los usuarios (ENS, RGPD, LPOD,…)
- ☆ La utilización de productos cualificados (CPSTIC) permite dotar a los sistemas de la Administración de mayor seguridad desde un enfoque metódico y objetivo.

- ☆ Para ampliar información: CCN-STIC 496, CCN-STIC serie 1000 (ccn.cni.es)

Gracias por su atención

movilsec.ccn@cni.es
cpstic.ccn@cni.es
ccn@cni.es

ccn.cni.es

Presentación elaborada por el equipo del Centro Criptológico Nacional para la FEMP.