DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Boletín protección de datos

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 24| Junio 2022

SEGURIDAD EN DISPOSITIVOS MÓVILES

Í N D I C E

SEGURIDAD EN DISPOSITIVOS MÓVILES

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN

Se considera **dispositivo móvil** al dispositivo electrónico de uso personal o profesional de reducido tamaño que permite la gestión (almacenamiento, intercambio y procesamiento) de información y el acceso a redes de comunicaciones y servicios remotos, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, *smartphones* (teléfonos móviles avanzados o inteligentes), *tablets* (tabletas) y agendas electrónicas, con independencia de si disponen de teclado físico o pantalla táctil.

En los últimos años, el desarrollo de estos dispositivos, junto con las tecnologías inalámbricas, ha revolucionado la forma de trabajar y comunicarse, situándolos como uno de los objetivos principales para los atacantes. Esto hace necesario plantearse cuál es la seguridad ofrecida por este tipo de dispositivos respecto a la información que gestionan, en especial dentro de los entornos corporativos.

El presente boletín tiene como objetivo ayudar a los usuarios de los sistemas de información de la Diputación de Valencia que para el desarrollo de sus labores cuenten con dispositivos móviles, a hacer un uso seguro de estos. Para ello, se ofrecerán un conjunto de recomendaciones de seguridad para evitar o, en su caso, mitigar posibles acciones dañinas.

"EL DESARROLLO DE LOS DISPOSITIVOS MÓVILES, JUNTO CON LAS TECNOLOGÍAS INALÁMBRICAS, HA REVOLUCIONADO LA FORMA DE TRABAJAR Y COMUNICARSE, SITUÁNDOLOS COMO UNO DE LOS OBJETIVOS PRINCIPALES PARA LOS ATACANTES".

BUENAS PRÁCTICAS EN LA CONFIGURACIÓN Y USO DE DISPOSITIVOS MÓVILES

HABILITAR LA PANTALLA DE BLOQUEO

Los dispositivos móviles modernos resultan muy atractivos para su sustracción o robo debido tanto a su valor económico, como al valor asociado a la información que almacenan. La pantalla de bloqueo es el principal mecanismo de defensa frente al acceso físico no autorizado al dispositivo móvil por parte de un potencial atacante. Con el objetivo de que el dispositivo móvil esté expuesto el menor tiempo posible frente a accesos no autorizados, incluso temporales, se recomienda **configurar el mismo para que el código de acceso sea solicitado inmediatamente tras apagarse la pantalla**, que debería de bloquearse automáticamente lo antes posible si no hay actividad por parte del usuario (por ejemplo, tras un minuto).

No obstante, aun bloqueado el dispositivo móvil, cabe la posibilidad de acceder a numerosas funcionalidades, como por ejemplo recibir y responder mensajes o llamadas de teléfono, recibir notificaciones de eventos y recordatorios, acceder a la cámara, modificar algunos ajustes, tener acceso a información de aplicaciones (*app*) concretas, etc. Esto también podría tener implicaciones en materia de seguridad, por lo que se recomienda **limitar lo máximo posible las funcionalidades disponibles en la pantalla de bloqueo si no se introduce el código de acceso.**

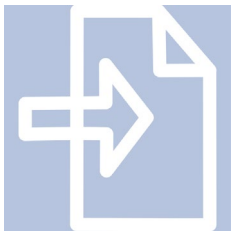
CIFRAR EL DISPOSITIVO

Las capacidades que permiten cifrar la memoria del dispositivo móvil son imprescindibles frente al acceso físico no autorizado al mismo por parte de un tercero, ya que, en caso contrario, sería posible extraer el contenido del chip de memoria del dispositivo móvil y tener acceso a toda la información almacenada.

Se recomienda **hacer uso de las capacidades nativas de cifrado del dispositivo móvil,** con el objetivo de proteger todos los datos e información asociadas al usuario u organización almacenados en el mismo.

En caso de que el dispositivo móvil disponga de una ranura para una **unidad de almacenamiento externa**, normalmente basada en la utilización de tarjetas de memoria SD, se recomienda hacer uso de capacidades de cifrado que permitan proteger también los contenidos de dicha unidad externa de almacenamiento. En muchas ocasiones no es posible cifrar dichos contenidos, por lo que **se recomienda no almacenar ningún dato o información sensible en la tarjeta SD, como por ejemplo documentos corporativos.**

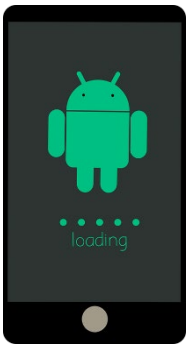
REALIZAR COPIAS DE SEGURIDAD



La protección de la información y los datos almacenados y gestionados por el dispositivo móvil debe de extenderse frente a escenarios de pérdida o robo del mismo, así como frente a daños en el *hardware* que no permitan acceder a los contenidos existentes en su unidad de almacenamiento principal (o en las unidades externas).

Para evitar la pérdida de los datos, el usuario debe realizar **copias de seguridad (*backups*) periódicas, y preferiblemente automáticas**, de todos los contenidos del dispositivo móvil que se desea proteger y conservar.

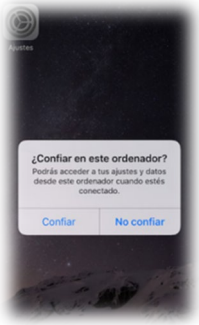
ACTUALIZAR EL SISTEMA OPERATIVO Y LAS APLICACIONES



Los dispositivos móviles disponen de un sistema operativo móvil (*Android, iOS*, etc.), también denominado *firmware*, que proporciona todas las funcionalidades existentes por defecto, y que también incluye un conjunto de aplicaciones móviles que han sido instaladas por defecto por el fabricante del sistema operativo, del dispositivo o del operador de telecomunicaciones.

Se recomienda **tener el sistema operativo siempre actualizado en el dispositivo móvil**. Asimismo, se recomienda **disponer siempre de la última actualización de todas las *apps* instaladas en el dispositivo móvil**. La última versión tanto del sistema operativo como de las *apps* **soluciona vulnerabilidades públicamente conocidas** y, por tanto, reduce significativamente la exposición del dispositivo frente a ataques.

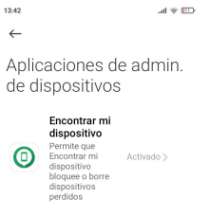
CUIDADO CON LAS CONEXIONES A TRAVÉS DE USB



Los puertos de carga y sincronización de los dispositivos móviles permiten la conexión por cable mediante un puerto USB a un ordenador o enchufe. Esto permite, de una parte, la transmisión de energía eléctrica para llevar a cabo la carga de la batería del dispositivo móvil, y de otra, establecer comunicaciones de datos. Los atacantes han empleado esta funcionalidad dual para comprometer los dispositivos móviles a través de la conexión de datos, haciéndose pasar por una estación de carga en lugares públicos. Mediante este ataque es posible extraer datos personales almacenados en el dispositivo móvil, así como llevar a cabo acciones más dañinas, como la instalación de apps dañinas.

Se recomienda **no conectar el dispositivo móvil a puertos USB desconocidos y no aceptar ninguna relación de confianza si no se tiene constancia de estar conectando el dispositivo móvil a un ordenador de confianza**.

GESTIÓN REMOTA DEL DISPOSITIVO MÓVIL



Los dispositivos móviles modernos permiten a cualquier usuario localizar la ubicación actual de su dispositivo móvil, bloquearlo en caso de encontrarse desbloqueado, hacer que suene para identificar su ubicación cercana, eliminar remotamente los datos almacenados en el mismo, etc.

Se recomienda al usuario **familiarizarse con las capacidades de gestión remota del dispositivo móvil** y su plataforma móvil asociada, y **comprobar el correcto funcionamiento** de este servicio y de toda su funcionalidad antes de que sea necesario hacer uso de las mismas en un escenario real tras la pérdida o robo del dispositivo móvil.

CONEXIÓN A REDES WI-FI

El interfaz Wi-Fi es probablemente el mecanismo de comunicación más utilizado en la actualidad en los dispositivos móviles a la hora de intercambiar datos y acceder a servicios y aplicaciones remotas.

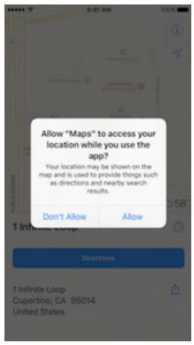
Se recomienda **no conectar el dispositivo móvil a redes Wi-Fi públicas abiertas** que no implementan ningún tipo de seguridad. Aunque su utilización no tenga ningún coste asociado, se está poniendo en riesgo la información personal del usuario. La utilización de esas redes permite a un potencial atacante interceptar y manipular todo el tráfico intercambiado por el dispositivo móvil.

CUIDADO CON LAS APLICACIONES MÓVILES QUE SE DESCARGAN

Los dispositivos móviles como los *smartphones* son considerados inteligentes porque, entre otros motivos, disponen de la capacidad de extender las funcionalidades existente por defecto mediante la instalación de nuevas aplicaciones móviles (*apps*).

Se recomienda **no instalar ninguna *app* que no sea estrictamente necesaria para el desarrollo de las tareas encomendadas en la organización** y, en caso de descargarla, que provenga **de una fuente de confianza, como por ejemplo los mercados oficiales de *apps*.** Aunque se han dado varios casos de código dañino tiendas oficiales, los controles existentes hacen que la probabilidad de infección sea menor que en otras plataformas móviles, y una vez detectado, es eliminado del mercado lo antes posible.

ADECUADA GESTIÓN DE LOS PERMISOS DE LAS *APPS*

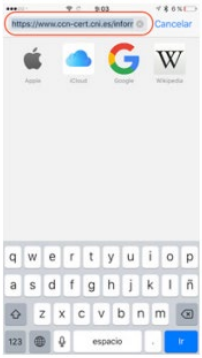


Para obtener acceso funcionalidades adicionales, las *apps* solicitan a menudo permisos al usuario, por ejemplo, para acceder a sus contactos, a su calendario, a componentes *hardware* del dispositivo móvil, como la cámara o el micrófono o a las fotos. Los permisos se solicitan al usuario en el momento de la instalación de la app o durante su ejecución, en el momento de hacer uso de cierta funcionalidad para la que un permiso concreto sea necesario.

Se recomienda **no otorgar permisos innecesarios o excesivos** a las apps, limitando así los datos y la funcionalidad a la que estas tendrán acceso. Para ello, es necesario que previamente el usuario entienda por qué una app solicita un permiso determinado y para qué es necesario dicho permiso dentro de la funcionalidad proporcionada por la *app*.

NAVEGACIÓN WEB SEGURA

Es muy habitual que los dispositivos móviles sean utilizados para tareas de navegación web.



Se recomienda, siempre que sea posible, **hacer uso del protocolo HTTPS** mediante la inserción del texto "https://" antes de introducir la dirección web del servidor con el que se desea conectar.

Desafortunadamente, por defecto, la barra de dirección de los navegadores web de los dispositivos móviles modernos tiende a minimizar la información mostrada al usuario, destacando únicamente el dominio con el que se ha establecido la conexión. Para poder obtener todos los detalles del servidor web y del recurso accedido, así como verificar si el método de conexión empleado es HTTPS (verificar que aparece un candado no siempre es suficiente), puede ser necesario seleccionar la barra de dirección y desplazarse hacia la izquierda para visualizar todos los detalles.

ESPECIAL CIUDADO CON EL CORREO, SMS Y SERVICIOS DE MENSAJERÍA

A través de estos servicios es posible recibir mensajes con enlaces web o adjuntos que albergan código dañino, con el objetivo de infectar y comprometer el dispositivo móvil del usuario víctima. El uso de enlaces dañinos es una de las técnicas más utilizadas para conseguir ejecutar código en el dispositivo móvil de la víctima o bien para obtener información de la misma.

Los ataques basados en enlaces maliciosos distribuidos a través de las *apps* de mensajería se suelen referenciar como *SMiShing*, y también incluyen mensajes atractivos, sugerentes o sobre los que el usuario debería llevar a cabo una acción urgente.

El consejo más eficaz para identificar mensajes dañinos es el **sentido común.** Esto significa que **cualquier síntoma o patrón fuera de lo considerado normal o habitual debe despertar la sospecha del usuario**. Un patrón o síntoma irregular puede significar: recibir un mensaje de un remitente no conocido, recibir un mensaje que solicite información personal, que el contenido del mensaje sea demasiado atractivo como para ser cierto, etc.

DEBER DE INFORMAR EN CASO DE INCIDENTE RELACIONADO CON EL DISPOSITIVO

Debe **informarse inmediatamente al responsable de seguridad de la organización** en el caso de perder o extraviar el dispositivo móvil, al igual que si se identifica cualquier comportamiento anómalo o sospechoso al hacer uso del mismo.

"LA CONCIENCIACIÓN, EL SENTIDO COMÚN Y LAS BUENAS PRÁCTICAS EN LA CONFIGURACIÓN Y EL USO DE LOS DISPOSITIVOS MÓVILES CONSTITUYEN LA MEJOR DEFENSA PARA PREVENIR Y DETECTAR ESTE TIPO DE INCIDENTES Y AMENAZAS".

MATERIAL COMPLEMENTARIO

- Informe: "Dispositivos móviles. Informe de buenas prácticas" (CCN). Consulta el informe en este enlace.
- Guía: "Privacidad y Seguridad en Internet" (AEPD). Consulta la Guía en este enlace.
- "¿Trabajas desde tu dispositivo móvil? ¡Implementa las mismas medidas de seguridad que en tu oficina!" (INCIBE). Consulta el post en este enlace.
- "Cómo prevenir incidentes en los que intervienen dispositivos móviles" (INCIBE). Consulta el post en este enlace.
- "Decálogo de buenas prácticas en seguridad móvil" (INCIBE). Consulta el post en este enlace.
- Guía: "Dispositivos móviles personales para uso profesional (BYOD)" (INCIBE). Consulta la Guía en este enlace.
- Política: "Uso de dispositivos móviles no corporativos" (INCIBE). Consulta este enlace.
- Dosier: "Protección en movilidad y conexiones inalámbricas" (INCIBE). Consulta el dosier en este enlace.
- "Protege tu móvil iOS y Android con 5 consejos" (OSI). Consulta este enlace.

NOTICIAS

- **Se publica Real Decreto 311/2022, de 3 de mayo, por el que se regula el nuevo Esquema Nacional de Seguridad (ENS).**

  El nuevo ENS no pretende ser un cambio disruptivo, sino que tiene cierto carácter continuista pero actualizado. Esta actualización se centra en algunos pilares fundamentales: alinear el ENS con el nuevo marco normativo de referencia; introducir la capacidad de ajustar los requisitos del ENS a necesidades específicas, determinados colectivos o determinados ámbitos tecnológicos; actualizar los principios básicos, los requisitos mínimos y las medidas de seguridad; perfeccionar el capítulo de "Prevención, detección y respuesta a incidentes de seguridad"; en general, clarificar, precisar, homogeneizar, simplificar y actualizar diferentes aspectos. Destaca la inclusión de la profesionalización de los roles a quienes corresponde velar por la seguridad de la información, al igual que el Reglamento Europeo de Protección de Datos introdujo la figura del Delegado de Protección de Datos. Es decir, se exige la formación, cualificación y dedicación de estos roles.

  Consulta la norma en este enlace.
  Consulta las infografías publicadas por el CCN en este enlace.

- **Nueva sección sobre salud y protección de datos en la web de la AEPD.**

  La nueva sección está compuesta por siete apartados que recogen desde información general sobre el tratamiento de los datos de salud y cómo ejercer el derecho de acceso a la historia clínica a cuestiones relacionadas con la investigación médica o las brechas de datos personales.

  Consulta este enlace.