CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

BUENAS PRÁCTICAS EN DISPOSITIVOS MÓVILES

Documento Público

septiembre de 2020

GENERALITAT VALENCIANA
Conselleria d'Hisenda i Model Econòmic

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Fondo Europeo de Desarrollo Regional

Una manera de hacer Europa

UNIÓN EUROPEA

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como
una apuesta de la Generalitat Valenciana por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Índice de contenidos

1. Introducción y objetivos

Las nuevas tecnologías, en su constante evolución, han permitido que se desarrollen nuevas herramientas para desempeñar labores profesionales de forma más eficaz. Se ha evolucionado, del ordenador como principal herramienta de trabajo, a utilizar dispositivos móviles como smartphones o *tablets* en entornos de trabajo donde la movilidad es fundamental.

Sin embargo, esa **movilidad conlleva unos riesgos** asociados a la posibilidad de pérdida o robo del dispositivo, produciéndose una pérdida de confidencialidad de la información contenida en el mismo.

El presente documento pretende recopilar una serie de recomendaciones básicas o **buenas prácticas de uso de *smartphones* y *tablets*** con el fin de aportar unas medidas de seguridad adecuadas para que la información almacenada en los dispositivos permanezca segura. Dichas recomendaciones serán personalizadas para los sistemas operativos más extendidos en este tipo de dispositivos: **Android**[1] e **iOS**[2].

1 *https://www.android.com/*
2 *https://www.apple.com/es/ios/*

2. Buenas prácticas

A continuación se enumerarán las medidas disponibles que se pueden llevar a cabo para incrementar la seguridad en los dispositivos móviles para cada uno de los sistemas operativos de uso más frecuente.

2.1. Seguridad Lógica

2.1.1 Bloqueo por contraseña

La gran mayoría de dispositivos dispone de medidas de bloqueo al entrar en modo suspendido. Este recurso garantiza que el acceso al uso del terminal solo puede efectuarse por la persona autorizada que conoce la clave. En caso de extravío o robo, la única manera de poder utilizar el dispositivo es restaurando los valores de fábrica, por lo que toda la configuración y datos almacenados se perderían.

Existen varios métodos para restringir el uso del dispositivo. Éstos varían en función del fabricante. Los más utilizados **son la contraseña con pin de 4 dígitos, contraseña alfanumérica o patrón de desbloqueo**.

Es importante, igualmente, configurar el terminal para que pasado **un tiempo de inactividad pase automáticamente a modo de suspensión y se active el bloqueo de la pantalla**. Si no se usara esta medida, la técnica de bloqueo perdería prácticamente toda su efectividad.

2.1.1.1 Bloqueo por contraseña en Android

En terminales con Android, para añadir una contraseña o patrón de desbloqueo se deben seguir los siguientes pasos:

Dentro del menú principal seleccione **Ajustes**, y busque el apartado de **Pantalla bloqueo y seguridad** después acceda a **Tipo de bloqueo de pantalla.**

En dicho apartado se podrá activar dicha protección de pantalla que podrá ser, a través de un patrón de movimiento que tendrá que realizar con el dedo en la pantalla, un pin numérico de 4 cifras, una contraseña de 4 caracteres y en algunos modelos de dispositivos se puede hacer uso de la huella digital.

En este mismo apartado también se puede configurar cuando se desea que se bloquee el dispositivo, si de manera inmediata o pasados unos minutos tras un periodo de inactividad

Se recomienda no mostrar visiblemente en nuestra pantalla nuestro pin, contraseña o patrón de desbloqueo mientras desbloqueamos nuestro terminal para evitar que un tercero pueda vernos mientras lo hacemos, para ello en este apartado de Seguridad se puede desactivar esta opción.

En algunas *tablets* para configurar una pantalla de bloqueo se puede hacer en **Ajustes/Ubicación y Seguridad/Configurar pantalla de bloqueo.** Al hacer clic se obtendrán las opciones de poner un patrón de movimiento, un pin o una contraseña.

2.1.1.2 Bloqueo por contraseña en iOS

En iPhones, o iPads se puede añadir una contraseña de acceso al dispositivo de la siguiente forma:

Dentro del menú principal navegue hasta **Ajustes,** y una vez dentro seleccione el apartado **General**, allí seleccione **Bloqueo con código** o **Touch Id y código dependiendo del modelo** donde se puede añadir un pin de 4 números de forma que cada vez que se acceda a nuestro dispositivo se deberá marcar dicho código.

Se puede también activar un campo (**Borrar datos**) donde tras marcar erróneamente determinadas veces un código, el contenido del dispositivo se borrará de forma inmediata, pero es algo que no se recomienda. Es importante además, evitar que al teclear el pin para acceder al dispositivo éste sea visionado por un tercero.

En **Ajustes/General** se puede activar bloqueo automático y elegir un tiempo (se recomienda 5 minutos) tras el cual si el dispositivo ha permanecido inactivo se bloquea de manera automática. El dispositivo no debe tener periodo de gracia para acceso sin clave. Así que en **Ajustes/General** en **Bloqueo con código** se debe tener en la opción **Solicitar** el valor INMEDIATAMENTE.

2.1.2 Cifrado de la memoria

Esta práctica se suele complementar con la técnica anterior. Consiste en cifrar la memoria de almacenamiento, haciendo imposible la copia o extracción de datos si no se conoce la contraseña de desbloqueo.

Según el modelo, se permite **cifrar tanto la memoria interna** como **la memoria de almacenamiento externo,** como son las tarjetas de memoria flash. Una vez cifrado, solo se podrá acceder a los datos almacenados al encender el dispositivo con la contraseña de bloqueo de pantalla.

Si no se conociese la clave sería muy difícil recuperar la información, aunque se utilicen técnicas forenses de extracción y copia de datos. La única forma posible sería con técnicas de fuerza bruta, que consisten en probar automáticamente todas las combinaciones posibles de contraseña, hasta encontrar aquella que permite el acceso.

Por tanto, es importante que para que este ataque no pueda llevarse a cabo, se utilice una contraseña compleja, que combine letras con dígitos, mayúsculas y caracteres especiales.

2.1.2.1 Cifrado de la memoria en Android

Android dispone de un sistema de cifrado del sistema de archivos del dispositivo a partir de la versión Android 3.0 Honeycomb.

Requiere que el usuario introduzca una contraseña o pin (en este caso no podremos poner como bloqueo por pantalla un patrón de movimiento ya que no está permitido que se use para cifrar la memoria) como bloqueo de pantalla que se utilizará para generar una clave que se usa para cifrar el sistema de archivos.

Es importante elegir una contraseña robusta que incluya letras y números para que la clave de cifra que se genere sea igualmente robusta. Para activar el cifrado del dispositivo se seguirán los siguientes pasos:

En **Ajustes**, se navegará hasta **Seguridad** y se debe activar la opción de **Cifrar dispositivo**. Se podrá cifrar cuentas, ajustes, aplicaciones descargadas y sus datos, multimedia y otros archivos. Una vez cifrado el dispositivo, se necesitará un pin o contraseña para descifrarlo cada vez que se encienda.

Es importante señalar que una vez cifrado el dispositivo el rendimiento del dispositivo se puede ver reducido y no es posible volver a dejarlo como estaba salvo que se restaure de fábrica.

2.1.2.2 Cifrado de la memoria en iOS

En iOS al fijar un código de acceso el dispositivo protege por defecto la información de las aplicaciones mediante una clave de cifra derivada de este código. Si tenemos activado el código de bloqueo, Apple lo utiliza junto a una clave de 256 bits única almacenada en el hardware del dispositivo para cifrar nuestros datos, como el correo electrónico.

Ninguna persona sin autorización podrá por tanto extraer información personal del dispositivo Para asegurarnos de que ésto ocurre se hará lo siguiente: En Ajustes/General/Bloqueo con código debe mostrarse el mensaje "La protección de datos está activada" en la parte inferior de la ventana.

2.1.3 Borrado remoto

Con esta práctica se podrán borrar los datos del dispositivo y restaurarlos a los valores de fábrica, todo ello de forma remota. Puede ser muy importante tener a mano este recurso en caso de pérdida o robo del dispositivo, en el supuesto de que la información almacenada sea sensible. Esta función depende del tipo de dispositivo, del fabricante o de la operadora, y es posible que el servicio sea de pago.

2.1.3.1 Borrado remoto en Android

Google ofrece un servicio de eliminación remota de datos de un dispositivo móvil para Google Apps for Business, Google Apps for Education y Google Apps for Government;

si su usuario ha configurado Google Sync en un dispositivo móvil compatible o en un dispositivo Android que tenga instalada la aplicación Política de dispositivos de Google Apps, se puede usar el panel de control de Google Apps para eliminar los datos del dispositivo de forma remota.

El borrado suprime todos los datos almacenados en el dispositivo (correo, calendario, contactos…etc.) pero no elimina los almacenados en la tarjeta SD del dispositivo. Para poder borrar un dispositivo de forma remota, primero tenemos que localizar el dispositivo para ello deben cumplirse una serie de condiciones:

- Haber añadido una **cuenta de Google** en el dispositivo, con lo cual, ya tendremos activado por defecto "Encontrar mi dispositivo". Además, tiene que tener la **sesión iniciada**.
- Tiene que **estar encendido**.
- **Conectado a una red de datos** móviles o WI-FI.
- Tiene que tener **activada la ubicación**.

Si disponemos de otro dispositivo Android, podemos instalar la aplicación "Encontrar mi dispositivo", disponible en la tienda **Play Store**.

Otra opción es acceder a la siguiente web[3], desde otro dispositivo o desde un ordenador y seguir los siguientes pasos:

1. Aquí debemos **iniciar sesión en la cuenta de Google** que sabemos que está activa en el dispositivo perdido/robado. Si tenemos varios dispositivos configurados con esa cuenta de Google, debemos elegir el dispositivo que queremos localizar, en la parte superior de la pantalla.

2. El **teléfono perdido recibirá una notificación**.

3. En el **mapa podremos ver la ubicación aproximada** de dónde se encuentra el dispositivo en este momento o de su última ubicación conocida.

4. Ahora debemos **hacer clic en "Habilitar bloqueo y borrado"**, para decidir qué queremos que suceda:

   * **Reproducir un sonido**, con lo que hacemos que el teléfono suene a máximo volumen durante 5 minutos, aunque esté en silencio o vibración.

   * **Bloquear dispositivo**, con lo que hacemos que se bloquee con el PIN, patrón o contraseña que tengamos establecido, y en caso de que no hubiéramos configurado ninguno, podemos hacerlo en este momento.

   * **Borrar dispositiv**o, para que elimine definitivamente todos los datos

3 https://www.google.com/android/find

del teléfono, aunque puede ser que no elimine los datos de la tarjeta SD. Pero si usamos esta opción, después ya no podremos utilizar Encontrar mi dispositivo. Además, si encuentras el dispositivo después de haber borrado los datos, es posible que necesites la contraseña de tu cuenta de Google para poder volver a usarlo.

2.1.3.2 Borrado remoto en iOS

Apple ofrece la función "**Buscar mi iPhone**"[4] , aplicación gratuita que te permite desde otro iPhone, iPad o iPod Couch, o utilizando un navegador Web para Mac o PC con una sesión iniciada en www.icloud.com15 varias opciones, entre ellas el borrado de todo el contenido y los datos del dispositivo restaurando los ajustes de fábrica.

Para poder usar sus características, la función "Buscar mi iPhone" debe estar activada en los ajustes de iCloud en tu dispositivo.

Dicha función solo puede estar activada en una cuenta. Para activar dicha función se debe acceder a **Ajustes/iCloud y activar "Buscar mi iPhone"**.

2.1.4 Copias de seguridad

Si la información utilizada en el dispositivo es importante, y su pérdida ocasionara graves problemas, entonces sería conveniente utilizar alguna solución de copias de seguridad.

Hay programas que sincronizan los datos almacenados con el ordenador de escritorio, o en alguna aplicación online ofrecida por el fabricante, de forma que los datos están siempre disponibles y actualizados. En esta página[5] se pueden encontrar herramientas para hacer copias de seguridad.

En caso de pérdida del terminal, la información seguiría estando disponible y a salvo. Se recomienda que si se utilizan este tipo de opciones, de sincronizar nuestros datos con alguna aplicación online externa a nuestra organización, no se sincronice la información confidencial si la hubiera, puesto que dejaría de 'estar en nuestras manos'. Lo recomendable es encontrar soluciones de copias de seguridad controladas por la organización, para que la información no viaje fuera de ella.

2.1.4.1 Copias de seguridad en android

Google no dispone de un servicio de copias de respaldo de los archivos de datos o multimedia del dispositivo, para ello habría que usar aplicaciones de terceros. Sin embargo sí permite copiar los ajustes del dispositivo (contraseñas de las redes WiFi, favoritos, datos de aplicaciones, opciones de configuración) en los servidores de Google. Los pasos a seguir son los siguientes:

- En **Ajustes/Privacidad** marcar la opción de **Copiar mis ajustes**. En algunas tablets tendremos que dirigirnos a **Ajustes/Privacidad** y marcar la opción de **Hacer copia de seguridad de la cuenta**.

4 https://apps.apple.com/es/app/buscar-mi-iphone/id376101648
5 https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=124

2.1.4.2 Copias de seguridad en iOS

A través de iCloud e iTunes se pueden realizar copias de seguridad de la mayoría de los datos de tu iPhone o iPad (fotos, ajustes del dispositivo como cuentas de correo o contactos, mensajes etc.).

Los pasos a seguir para que iCloud realice de manera automática una copia de seguridad de los datos más importantes de tu dispositivo son los siguientes:

- Ir a **Ajustes/iCloud/Almacenamiento y copias**

La copia de seguridad se ejecutará a diario siempre y cuando su dispositivo:

- Esté conectado a Internet vía WiFi.
- Esté conectado a una fuente de alimentación.
- Tenga la pantalla bloqueada.

Es posible hacer una copia de seguridad de manera manual siempre que su dispositivo esté conectado a Internet vía WiFi seleccionando "Realizar copia de seguridad ahora" en **Ajustes/iCloud/Almacenamiento y copias**.

2.2. Los peligros del malware

El uso cada día más frecuente de smartphones y tablets ha derivado en que la creación de malware apunte hacia estas plataformas. Hoy día el riesgo de que un smartphone pueda ser infectado por un virus es una realidad.

Éstos se basan principalmente en el robo de documentos, contraseñas, datos bancarios e información personal. Por eso es conveniente adoptar unas medidas de seguridad para evitar en la medida de lo posible infecciones de malware que haga peligrar la confidencialidad, integridad y disponibilidad de la información.

Se recomiendan las lecturas de nuestras campañas de concienciación "Seguridad en Aplicaciones móviles"[6] y "Seguridad en dispositivos móviles"[7].
A continuación algunos consejos importantes sobre ésto.

2.2.1 Fuentes confiables

El principal problema de infecciones en dispositivos móviles es por causa de la instalación de programas desde fuentes desconocidas.

Es muy importante instalar aplicaciones únicamente desde los repositorios oficiales del dispositivo, como App Store y Google Play, para iPhone/iPad y Android

6 https://concienciat.gva.es/tips_de_seguridad/seguridad-en-aplicaciones-moviles/
7 https://concienciat.gva.es/tips_de_seguridad/seguridad-en-dispositivos-moviles/

respectivamente.

Se debe evitar siempre instalar aplicaciones descargadas directamente de P2P, o foros. Se corre el serio riesgo de que estos programas contengan algún troyano y tras su instalación, infecten el dispositivo.

2.2.2 Jailbreak/root

Los términos Jailbreak o root de un dispositivo se refieren a conceder privilegios de administración a las aplicaciones, saltándose la jaula de protección que tiene por defecto los sistemas operativos.

Esta característica puede añadir funcionalidades extra al dispositivo, pero también es un riesgo extra al que se expone, ya que se está eliminando la barrera de protección que sin jailbreak o root se mantiene.

Salvo que sea absolutamente necesario para el funcionamiento de una aplicación concreta, se desaconseja habilitar esta característica a los dispositivos.

2.2.3 Solo las aplicaciones necesarias

Llenar el dispositivo de aplicaciones innecesarias no solo ralentiza su funcionamiento, sino que aumenta el riesgo de que una de estas aplicaciones tenga una vulnerabilidad que pueda ser aprovechada por un atacante y conseguir el control del dispositivo.

Por eso es recomendable desinstalar toda aplicación que no sea estrictamente necesaria para el desempeño del dispositivo, y así minimizar el riesgo de exposición por una aplicación vulnerable. Además es importante leer los permisos y condiciones tienes que aceptar antes de instalar una aplicación y comprobar la reputación de la misma.

2.2.4 Protección antivirus

Se recomienda disponer de un antivirus en el dispositivo móvil como medida extra de protección contra el malware. En esta página[8] se pueden encontrar diferentes antivirus, muchos de ellos disponibles también para dispositivos móviles.

2.2.5 Actualizaciones de software

Los sistemas operativos de los dispositivos incluyen un sistema de actualización de aplicaciones. Mediante una notificación, informan que existe una nueva versión de una aplicación instalada. Estas actualizaciones, además de añadir funcionalidades, corrigen fallos de seguridad.

Siempre que el sistema notifique de una actualización disponible, se **debe aceptar y aplicar la nueva versión**. Manteniendo el sistema actualizado se evitan posibles infecciones por aplicaciones vulnerables.

8 https://www.osi.es/es/herramientas-gratuitas?combine=&herramienta_selec%5B%5D=124&herramienta_selec%5B%5D=115

2.2.5.1 Actualizaciones software Android

Para comprobar que nuestro sistema esta actualizado se navegará hasta **Ajustes/Acerca del teléfono/Actualizaciones de software** y se comprobará que está marcada la opción de Comprobación programada o Descarga automática.

Se puede comprobar de forma manual si se pulsa en **Comprobar ahora** o **Descarga manual** si nuestro sistema esta completamente actualizado.

2.2.5.2 Actualizaciones software iOS

En **Ajustes/General/Actualización de software** se debe obtener el mensaje "El software está actualizado".

2.3 Otras recomendaciones

2.3.1 No almacenar información sensible

La información más delicada de la empresa u organización no debe ser almacenada en dispositivos móviles aunque estén cifrados puesto que los dispositivos móviles suponen riesgos mayores. Si se ha de acceder a dicha información crítica desde un dispositivo móvil **debe hacerse de forma online a servidores seguros**.

2.3.2 Wifi Públicas

Las redes inalámbricas de uso público, o compartido, como las disponibles en hoteles o cafeterías pueden suponer un riesgo. A pesar de que tenga contraseña para poder utilizarse, un atacante podría conectarse y capturar el tráfico de todas las personas que se encuentran conectadas a esa red inalámbrica. Podría entonces analizar el tráfico capturado y recopilar contraseñas o datos confidenciales.

Si se va a hacer uso de redes inalámbricas de uso público, se recomienda no acceder a ningún servicio que requiera contraseña, realizar operaciones bancarias o descargar documentos confidenciales.

2.3.3 Desactivar comunicaciones inalámbricas

Es muy importante **desactivar las redes inalámbricas si no se van a utilizar** a corto plazo. Las redes más usuales suelen ser WIFI, Bluetooth, o infrarrojos. Es posible realizar ataques contra redes inalámbricas, utilizando puntos de acceso falsos, y engañando al dispositivo para que se conecte automáticamente a una red de supuesta confianza. El usuario navegaría entonces sin tener constancia de que el tráfico está siendo monitorizado por un atacante.

A continuación se indica cómo desactivar el Bluetooth.

2.3.3.1 Desactivar Bluetooth. Android

En **Ajustes/Conexiones y redes** se puede desactivar la opción para la conexión a través de Bluetooth. Se recomienda **activarlo únicamente cuando sea estrictamente necesario.**

2.3.3.2 Desactivar Bluetooth. iOS

En la pantalla de inicio haga clic en el **área de conexiones** situada en la parte superior de la pantalla y clic en el icono de **Gestionar conexiones**. Para desactivar el Bluetooth **desmarque la casilla de verificación Bluetooth**.

2.3.4 Cargadores públicos

Se han dado casos de **fugas de información** en dispositivos móviles por haber sido conectados en **cargadores públicos**.

Se debe evitar conectar el dispositivo por USB a cualquier ordenador público, como hoteles o cibercafés, y cualquier otro aparato que no tengamos total confianza en él. Ya que pueden haber sido manipulados para extraer información de cualquier dispositivo USB que se conecte.

2.4 Conclusiones

El uso tan extendido de **dispositivos móviles** ha hecho que se conviertan de manera activa en una herramienta más de nuestro trabajo, alojando en muchas ocasiones información corporativa crítica o valiosa, que en caso de ser interceptada, conllevaría grandes problemas de seguridad.

Dicho uso tan extendido de estos dispositivos ha hecho que los ciberdelincuentes lo vean como un nicho de mercado a explotar, y **a día de hoy, los dispositivos móviles se han convertido en uno de los focos principales ante ataques informáticos**. Es por todo ello por lo que, tanto los usuarios finales como empresas, deben poner todos los medios de los que disponen para implantar una estrategia de seguridad en movilidad con el objetivo de garantizar la integridad, confidencialidad y disponibilidad de la información corporativa.

Es importante conocer bien las opciones que cada fabricante nos ofrece, y aplicar una configuración de seguridad adecuada en aras de **bastionar el dispositivo móvil sin perder prestaciones**.

También es **importante saber** qué información **podemos almacenar o no en nuestro dispositivo** (evitar siempre información confidencial) y qué aplicaciones (las mínimas y necesarias) y de dónde las instalamos (siempre de fuentes fiables).

En definitiva, se insta a las empresas a que establezcan unos **criterios y procedimientos adecuados** para implantar una estrategia de seguridad en movilidad que conlleve sobre todo una correcta **formación y concienciación** tanto de **usuarios como de administradores**.

3. Contacto y consultas

En caso de desear ampliar la información sobre este u otros temas, o acceder a toda la oferta formativa del Centro de Seguridad TIC de la Comunitat Valenciana, es posible hacerlo en las siguientes direcciones:

https://www.csirtcv.gva.es/
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv