Guía de buenas prácticas en el uso corporativo de dispositivos móviles

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GENERALITAT VALENCIANA
CONSELLERIA DE HACIENDA Y ADMINISTRACIÓN PÚBLICA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-cv

CSIRT-cv es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, englobado dentro del III Programa de Servicios de Telecomunicaciones Avanzados Corporativos y de Comunicación con los Ciudadanos incluido en el Plan Estratégico Valenciano de Telecomunicaciones Avanzadas (PEVTA) del programa Avantic, como una apuesta de la **Generalitat de la Comunitat Valenciana** por la seguridad en la red.

Se trata de una iniciativa pionera al ser el primer centro de estas características que se crea en España para un ámbito autonómico.

Datos de contacto

CSIRT-cv Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/
Generalitat de la Comunitat Valenciana,
C/Cardenal Benlloch, 69 Entlo
46021 Valencia, España

Teléfono: +34-96-398-5300
Telefax: +34-96-196-1781
Email: csirtcv@gva.es
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

CSIRT-cv, dispone de un **catálogo de servicios**[1] donde se recogen las funciones y prestaciones que ofrece a todo su ámbito de actuación, diferenciado por colectivos. Estos recursos son gratuitos y se ampliarán gradualmente. Con ellos, **CSIRT-cv** espera contribuir de manera eficaz al correcto funcionamiento de las administraciones, PYMES y de sus servicios en favor de los ciudadanos.

Se sigue el patrón clásico de los Equipos de Respuesta ante Incidentes y unifica los servicios en tres grandes grupos en función del momento y la forma en la que actúa ante un incidente.

CSIRT-cv dentro de su catálogo de servicios ofrece ciertos servicios de valor añadido que aumentan los ya existentes y son independientes de la gestión de incidentes. Con éstos, brinda su experiencia para ayudar a mejorar la seguridad general de la organización identificando riesgos, amenazas y debilidades del sistema. Estos servicios contribuyen indirectamente a reducir la cantidad de incidentes.

Algunos de estos servicios de valor añadido son los servicios de **Formación y Concienciación** y, como parte de los mismos, **CSIRT-cv** decidió elaborar esta guía sobre buenas prácticas en dispositivos móviles enfocada sobre todo a entornos corporativos.

[1] http://www.csirtcv.gva.es/es/paginas/servicios-csirt-cv.html

Índice de contenido

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 cada uno de los tres sistemas operativos más extendidos en este tipo de dispositivos: **Android**[2], **iOS**[3] y **BlackBerry OS**[4].

[2] http://www.android.com/
[3] http://www.apple.com/es/ios/
[4] http://es.blackberry.com/services/

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: 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 **Seguridad**. En dicho apartado tiene la opción de **Cambio bloqueo pantalla,** donde podrá bien activar dicha protección de pantalla a través de un patrón de movimiento que tendrá que realizar con el dedo en la pantalla, un pin numérico de 4 cifras o bien una contraseña de 4 caracteres. 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*[5] 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.

[5] Por ejemplo la Samsung Galaxy Tab 10.1

2.1.1.2 Bloqueo por contraseña: 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** 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.

2.1.1.3 Bloqueo por contraseña: BlackBerry OS

Para BlackBerry los pasos a seguir para poner una contraseña son los siguientes:

BlackBerry permite poner contraseñas de entre 4 y 14 caracteres y rechaza ciertas combinaciones no seguras. Para configurar una contraseña hay que dirigirse en la pantalla principal a **Opciones**, seleccionar **Seguridad**, cambiar la opción de **Contraseña** a Activar, pulsar la tecla de **menú** y posteriormente hacer clic en **Guardar**. Se escribe la nueva contraseña, se confirma y se pulsa Aceptar. Para que se bloquee de manera automática, también en **Contraseña** se puede configurar el valor tras el cual se quiere que se bloquee automáticamente en **Bloquear después de:** se escoge un tiempo, se pulsa la tecla de **menú** y se pulsa en **Guardar**.

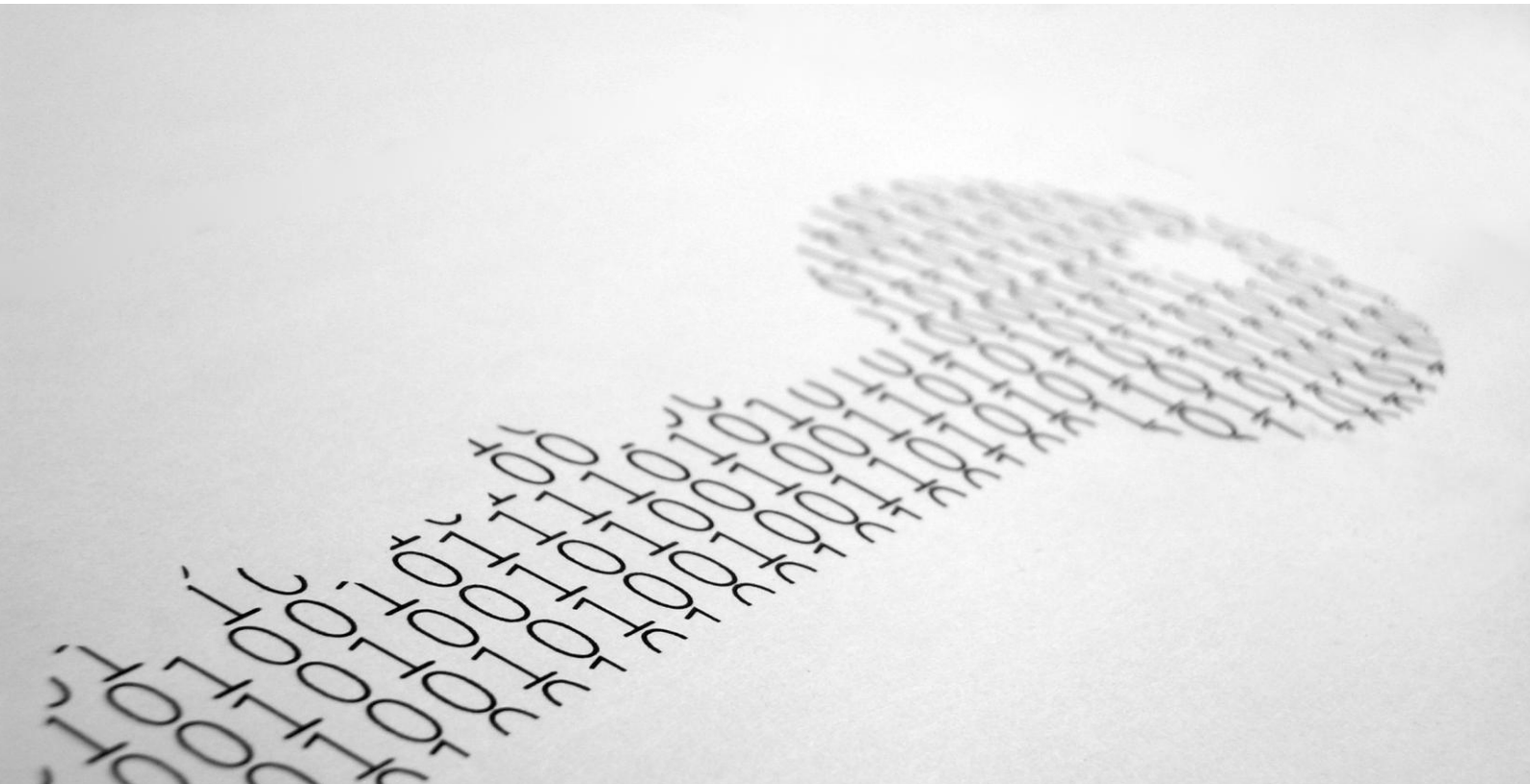
2.1.2 Cifrado de la memoria

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 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 no sería posible 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 sea muy difícil de 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: 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 utiliza 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 activa la opción **Encriptar teléfono**[6]

En algunas *tablets*[7] para cifrar el dispositivo se navegará a **Ajustes/Ubicación y seguridad/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

[6] El término correcto no sería Encriptar (meter algo en una cripta) sino Cifrar. Sin embargo es habitual encontrar en la literatura el termino Encriptar refiriéndose a Cifrar.
[7] Como la Samsung Galaxy Tab 10.1

2.1.2.2 Cifrado de la memoria: 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. 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.

2.1.2.3 Cifrado de la memoria: BlackBerry OS

En Blackberry es posible cifrar los archivos en la memoria del dispositivo aunque depende de la cantidad de la memoria disponible. Para poder cifrar nuestro sistema de ficheros es necesario haber configurado una contraseña para nuestro dispositivo. Los pasos a seguir serán los siguientes:

En la pantalla de inicio o en una carpeta se navegará a **Opciones** y se hará clic en **Seguridad**. Se irá a Cifrado y se cambiará el campo Cifrado a Activado. Para cifrar los datos en la memoria del dispositivo, se tiene que establecer el campo **Memoria** del dispositivo en Activado. Para cifrar los archivos almacenados en una tarjeta multimedia y en su dispositivo, hay que establecer el campo **Tarjeta multimedia** en Activado y se podrá llevar a cabo una de las siguientes opciones:

Para cifrar archivos mediante una clave de cifrado generada por el dispositivo, hay que cambiar el campo **Modo** a **Clave del Dispositivo**. Para cifrar los archivos mediante la contraseña del dispositivo, se cambiará el campo **Modo** a **Contraseña del dispositivo**. Para cifrar los archivos mediante una clave de cifrado y una contraseña de dispositivo, se cambiará el campo **Modo** a **Contraseña y clave del Dispositivo**. Para cifrar también los archivos multimedia como imágenes, canciones y videos, se establecerá el campo **Incluir archivos multimedia** en **Si**. Se pulsan las teclas **Menú** y **Guardar.**

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: Android

Google ofrece un **servicio de eliminación remota de datos de un dispositivo móvil**[8] solo para **Google Apps for Business**, **Google Apps for Education** y **Google Apps for Government**; si su usuario ha configurado **Google Sync**[9] en un dispositivo móvil compatible o en un dispositivo Android que tenga instalada la aplicación **Política de dispositivos de Google Apps**[10], 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.

Los pasos a seguir son los siguientes:

1. Iniciar sesión en su panel de control de Google Apps[11]
2. Clic en **Configuración** > **Móvil.**
3. En la pestaña "**Dispositivos**"[12] sitúese encima del usuario cuyo dispositivo quieras eliminar.
4. Clic en **Eliminación remota** del cuadro que aparece.
5. Confirmar haciendo clic en **Borrar datos del dispositivo.**

Los inconvenientes de este método son que si se tiene habilitada la configuración para realizar el borrado remoto de los dispositivos, los usuarios puede que por accidente los eliminen desde la página **Mis dispositivos**[13].

8 http://support.google.com/a/bin/answer.py?hl=es&answer=173390

9 http://support.google.com/a/bin/answer.py?answer=135937

10 http://www.google.es/support/a/bin/answer.py?&answer=1056433

11 http://www.google.com/support/a/bin/answer.py?answer=55955

12 http://www.google.com/support/a/bin/answer.py?answer=1408863#remote-wipe

13 http://support.google.com/mobile/bin/answer.py?&answer=1235372

2.1.3.2 Borrado remoto: iOS

Apple ofrece la función "**Buscar mi iPhone**"[14], 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.com[15] 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. Los pasos a seguir son los siguientes:

Activar "Buscar mi iPhone" mediante iCloud: Ir a **Ajustes/iCloud** y activar "Buscar mi iPhone"

Los requisitos de esta solución son los siguientes:

Tiene que estar registrado en iCloud[16].

Los sistemas de localización del móvil deberán estar activos para que se pueda usar dicha aplicación

No funciona si el dispositivo no tiene conexión a Internet, está apagado o se le hace un reseteo.

[14] http://itunes.apple.com/es/app/buscar-mi-iphone/id376101648?mt=8

[15] http://www.apple.com/es/icloud/what-is.html

[16] http://www.apple.com/legal/icloud/es/terms.html

2.1.3.3 Borrado remoto: BlackBerry OS

BlackBerry ofrece una aplicación gratuita, **BlackBerry Protect**[17] que permite eliminar la información del dispositivo[18] y de la tarjeta microSD desde el sitio Web de BlackBerry Protect [19] . Los requisitos del uso de esta aplicación son los siguientes:

- Necesita estar suscrito a BlackBerry ID[20].
- Los sistemas de localización del móvil deberán estar activos para que se pueda usar dicha aplicación.

Cabe destacar que BlackBerry Protect no es compatible con dispositivos que utilicen BlackBerry Enterprise Server (o Express). En este caso los administradores de la plataforma son los que podrían eliminar remotamente la información del dispositivo.

[17] http://es.blackberry.com/services/protect/
[18] http://www.todoenblackberry.com/2011/04/descarga-instala-y-configura-blackberry-protect-paso-a-paso/
[19] https://blackberryid.blackberry.com/bbid/login/
[20] https://blackberryid.blackberry.com/bbid/registration/registration_eula.seam?i=8565792

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 caso de pérdida de la 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: 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.**

2.1.4.2 Copias de seguridad: iOS

A través de iCloud e iTunes se pueden realizar copias de seguridad[21] 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.**

[21] http://support.apple.com/kb/HT1766?viewlocale=es_ES&locale=es_ES

2.1.4.3 Copias de seguridad: BlackBerry OS

BlackBerry ofrece un servicio de copias de seguridad del *smartphone*. Los pasos a seguir son los siguientes:

- Conectar el dispositivo a un ordenador y abrir **BlackBerry Desktop Manager.**
- Doble clic en **Copia de seguridad/restauración de archivos.**
- Seleccionar **Copia de seguridad** para realizar una copia de seguridad completa, o bien **Avanzado** para realizar una copia de seguridad de los datos que especifique.
- Se elige la ubicación donde se desea guardar el archivo de copia de seguridad y se hace clic en **Guardar.**

La recuperación de datos se hace de forma similar.

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**"[22] y "**Seguridad en dispositivos móviles**"[23]

A continuación algunos consejos importantes sobre ésto.

[22] http://www.csirtcv.gva.es/es/paginas/seguridad-en-aplicaciones-m%C3%B3viles.html
[23] http://www.csirtcv.gva.es/es/paginas/seguridad-en-dispositivos-m%C3%B3viles.html

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 o Google Play y App World*, para *iPhone/iPad o Android* y BlackBerry 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 la sección de **Utilidades**[24] de nuestro portal Web se pueden encontrar diferentes antivirus gratuitos, muchos de ellos disponibles también para dispositivos móviles.

[24] http://www.csirtcv.gva.es/es/paginas/antivirus.html

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.

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

2.2.5.2 Actualizaciones de software. iOS

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

2.2.5.3 Actualizaciones de software. BlackBerry OS

Para comprobar las actualizaciones del sistema, hay que acceder a través de **Opciones** a través de **Dispositivo**, se seleccionará **Actualización de software** y se siguen las instrucciones que aparecerán al ejecutar la aplicación. En caso de que el operador envíe alguna actualización, ésta aparecerá automáticamente.

En entornos corporativos con **BlackBerry Enterprise Server** serán los gestores de la plataforma los que decidirán sobre las actualizaciones del dispositivo.

Si se trata de actualizaciones de aplicaciones instaladas a través de App World, también saldrá una notificación que indicará la disponibilidad de una nueva versión para actualizar. En las actualizaciones de App World habrá que introducir el BlackBerry ID para que se puedan instalar.

2.3 Otras recomendaciones

Otras recomendaciones importantes que no se quieren dejar de mencionar, además del sentido común a la hora de usar los dispositivos móviles y pensar siempre en lo que se está haciendo, son las siguientes:

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 **Ajustes/General/Bluetooth** se deberá fijar la opción "NO". De esta forma aseguramos que nuestra conexión por Bluetooth está desactivada.

2.3.3.3 Desactivar Bluetooth. BlackBerry OS

En la pantalla de inicio haga clic en el **área de conexiones** sita 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. Pueden haber sido manipulados para extraer información de cualquier dispositivo USB al que se conecten.

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.

Ante cualquier duda, consulta o aclaración puede consultarnos a través nuestras vías de contacto indicadas al inicio.