Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Seguridad en dispositivos Android

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-9940-130716*
Edición:	*0*
Categoría	*Uso Interno*
Fecha de elaboración:	*13/07/2016*
N° de Páginas	*1 de 15*

1 TABLA DE CONTENIDOS

2 OBJETIVO

El objeto de este documento es aproximar a un usuario poco experimentado a la seguridad en dispositivos Android.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Pretende aportar las nociones básicas necesarias para entender el uso y configuración, desde el punto de vista de la seguridad, de los muy extendidos dispositivos Android. Este documento ayudará a los usuarios a como proteger la información gestionada por estos terminales, comprender el sistema de permisos de las aplicaciones que se instalan, mantener el terminal actualizado, realizar comunicaciones seguras, etc; en cualquier caso no se debe considerar como una política de uso corporativo.

Se debe tener en cuenta que los ejemplos aquí mostrados, aunque genéricos y válidos para la mayoría de las versiones Android, han sido elaborados basándose en la versión 4.4 del sistema operativo Android.

4 SEGURIDAD DE LA INFORMACIÓN

Hoy en día existen muchos más terminales móviles que PCs (Ordenadores Personales) y, sin duda, el sistema operativo más extendido para estos dispositivos es Android, llegando a aproximarse al 80% de cuota de mercado. En base a estos datos podemos extrapolar que existen más usuarios de Android que de cualquier otro sistema operativo móvil. Además, la mayor parte de estos dispositivos cuenta con conexión autónoma a Internet. Sin duda, esto supone que la cantidad de información que se almacena en estos sistemas, más la que es transmitida hacia o desde ellos, sea enorme. Toda esta información es susceptible, tal como sucede en cualquier otro sistema TI, de ser modificada, borrada o accedida de forma fraudulenta, por lo que es necesario aplicar una serie de medidas de protección.

A continuación vamos a exponer una serie de pautas para reforzar la seguridad de nuestro sistema Android ante accesos indeseados, tanto al sistema como a la información que en él se almacena y gestiona.

4.1 Protección frente al acceso físico

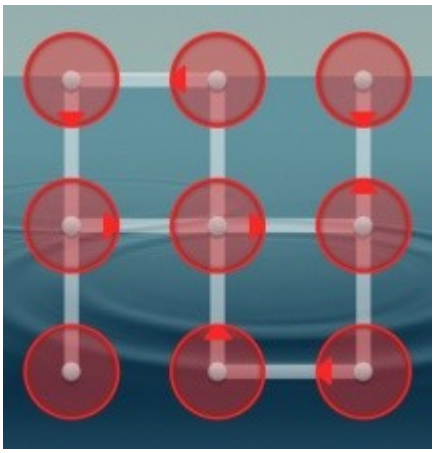
El primer nivel de seguridad en cualquier sistema TI es el acceso físico a los sistemas que contienen la información que se necesita proteger. Para este fin tenemos dos opciones básicas: el bloqueo por PIN asociado a la tarjeta SIM y el bloqueo de pantalla por inactividad (o bloqueo voluntario del usuario).

4.1.1 Bloqueo por PIN asociado a la tarjeta SIM

Este sistema de seguridad sólo es aplicable cuando el terminal es iniciado/reiniciado. Cuando el sistema completa el proceso de arranque nos solicita un código de activación SIM que nos ha proporcionado operador. Sin este código el terminal sólo nos permitiría la realización de llamadas a números de emergencia. Por desgracia, la mayoría de operadores usan PIN muy cortos (lo más común es que sean de 4 dígitos), lo que los hace vulnerables a ataques por adivinación. Una primera configuración de seguridad sería cambiar la clave por defecto de nuestra tarjeta SIM por una más robusta. Android lo permite dentro de Ajustes → Seguridad → Bloqueo de tarjeta SIM → Cambiar PIN tarjeta SIM. Esto nos permitirá establecer un PIN de hasta de 9 dígitos.

4.1.2 Bloqueo de pantalla

Disponemos de una segunda capa de bloqueo de pantalla por inactividad o por bloqueo voluntario del usuario. Este sistema es el más esencial desde el punto de vista de la seguridad ante accesos indeseados al dispositivo. Mientras que el bloqueo por PIN de tarjeta sólo es aplicable en el inicio del sistema, el bloqueo de pantalla nos permitirá que nuestro terminal esté activo, pero bloqueado, siempre que queramos. Incluso que se bloquee de forma automática. Al igual que el método anterior, este tipo de bloqueo impedirá el acceso a las funcionalidades del sistema y a la información almacenada en el mismo. Android permite dentro de Ajustes → Seguridad → Bloqueo de pantalla, configurar el sistema para que nos solicite un PIN para desbloquear el terminal. Además, podremos establecer un temporizador de uso, de tal forma que si nuestro terminal se encuentra inactivo durante X minutos, el sistema se bloquee automáticamente. Más aún, puesto que la seguridad no siempre está reñida con la facilidad de uso, Android nos permite establecer otros sistemas de desbloqueo: asociados a nuestro rostro o en base a un patrón previamente definido. De esta forma se facilita el uso de esta protección.



Hay que tener en cuenta que es muy importante no olvidar la clave o el patrón de desbloqueo, ya que en tal caso no se tendría acceso al sistema. Como último recurso si se ha olvidado alguno de éstos, puede ser necesario restaurar el sistema a los valores de fábrica.

4.1.3 Cifrado

Aunque los métodos anteriores nos protegen de forma efectiva ante accesos ocasionales de terceros al dispositivo, como último recurso ante una posible pérdida o substracción del dispositivo, puede ser conveniente la aplicación de una nueva capa de seguridad mediante el cifrado de los datos personales que se encuentren en el sistema. Este último punto puede ser muy recomendable, sobre todo en dispositivos corporativos que manejan documentación que legalmente debe estar protegida y cuya pérdida puede acarrear graves consecuencias, tanto económicas como de imagen.

Esta opción puede encontrarse en la ruta Ajustes → Seguridad → Encriptar teléfono. Hay que tener en cuenta ciertos detalles antes de tomar la decisión de cifrar el teléfono. Sin lugar a dudas, la más importante es que si olvidamos la clave de cifrado perderemos irreversiblemente todos los datos almacenados en el teléfono. *Llegados a este punto, tal vez deberíamos pensar en el uso de algunos sistemas de gestión de credenciales, como por ejemplo KeePass.* Otro detalle a tener en cuenta es que el cifrado ocasionará cierta perdida de rendimiento del dispositivo, ya que además de las tareas habituales, deberá cargar con el cifrado y descifrado de la información en cada acceso a ésta. Es necesario indicar que la opción de cifrado del dispositivo, no encripta realmente todo el dispositivo, ya que únicamente cifra la información del usuario almacenada en la ruta "/data," por lo que no debemos tener miedo a perder el dispositivo de forma irremediable si olvidamos la clave de cifrado. Seguiremos teniendo la opción de reiniciarlo a los valores de fábrica.

En caso de estar decididos a proteger nuestra información mediante el paso que se acaba de exponer, debemos asegurarnos (el sistema nos lo pide como requisito) de que tenemos habilitado un código PIN de acceso al terminal y que el dispositivo está conectado a una fuente externa, ya que el proceso de cifrado puede tardar varios minutos y sería catastrófico que el proceso fallara debido a que se le haya agotado la batería al terminal.

Durante el proceso, el sistema puede tener que reiniciarse varias veces y nos pedirá la clave de cifrado, que será la que nos pedirá cada vez que iniciemos el dispositivo para poder acceder a la información protegida por este método.

4.2 Protección frente a la pérdida de datos. "Copias de seguridad"

Mediante los tres pasos anteriores aplicados a un dispositivo Android podemos afirmar, aunque la seguridad nunca es un termino absoluto, que nuestro dispositivo está configurado de forma robusta ante intentos de accesos físicos no deseados. No obstante, la información es importante y "frágil", por lo que debemos protegerla de ataques lógicos o incluso de posibles errores involuntarios que nosotros mismos podemos cometer. Es frecuente, sobre todo cuando se trabaja con gran volumen de información, que se borren o modifiquen datos valiosos de forma accidental. Ante estas incidencias y otros riesgos actuales como el ransomware o la pérdida del dispositivo, la medida más efectiva es el mantenimiento de copias de seguridad periódicas de la información sensible.

Existen múltiples opciones para la realización de copias de seguridad en los dispositivos Android. Aquí vamos a ver las opciones más comunes: las copias usando Google y las copias a un sistema local sin necesidad de depender de terceros.

4.2.1 Copia de archivos de forma manual

Dentro de las copias locales lo más sencillo es la copia manual de archivos. Esto consiste simplemente en conectar nuestro terminal a un PC vía USB y copiar al ordenador los archivos de los que queramos hacer una copia.

Para restaurar estos datos simplemente se conectará el dispositivo de nuevo al PC y se copiarán a sus localizaciones los archivos previamente salvados.

4.2.2 Copia íntegra desde línea de comandos

Otra forma de copias sin intervención de terceros es mediante el uso de programas ADB (Android Debug Bridge) que permiten la copia íntegra del sistema. El programa ADB, disponible tanto en Windows como en Linux, nos permitirá realizar copias a distinto nivel e incluso cifrar las copias de seguridad realizadas. A continuación podemos ver algunos ejemplos de la utilización de estos comandos:

WINDOWS

- Realizando copia de seguridad

Descubrimos los dispositivos conectados:

C:\Users\siles>adb devices
098579c984984 device

Realizamos la copia completa en el archivo Android.ab

C:\Users\siles>adb backup -f Android.ab -all

Tras este ultimo comando el dispositivo nos pedirá confirmación y, si lo deseamos, una clave de cifrado para el archivo de copia generado. Como en cada paso que implique cierto tiempo para ser llevado a cabo, es recomendable realizarlo estando seguros que el proceso no será interrumpido por motivos ajenos a la tarea.

- Restaurando copia de seguridad

Descubrimos los dispositivos conectados:

C:\Users\siles>adb devices
098579c984984 device

Iniciamos la recuperación:

C:\Users\siles>adb restore Android.ab

De nuevo, en el dispositivo nos aparecerá una pantalla de confirmación para la restauración y, en su caso, nos pedirá la clave de cifrado con la que se realizó la copia de seguridad.

LINUX

- Realizando copia de seguridad

Instalamos los paquetes necesarios:

UBUNTU:
 # apt-get install android-tools-adb
FEDORA:
 # yum install android-tools

A partir de aquí el procedimiento es claramente similar al descrito para los sistemas Windows.

$ adb devices
List of devices attached
098579c984984 device

Realizamos la copia completa en el archivo Android.ab

$ *adb backup -f Android.ab -all*

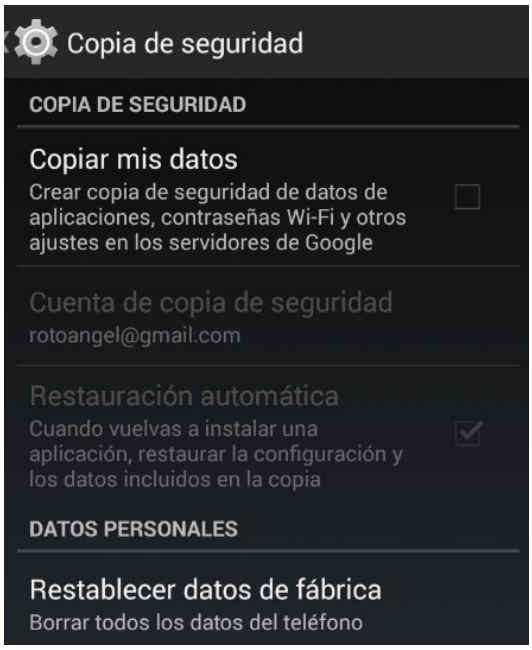
Tras este último comando el dispositivo nos pedirá confirmación y, si lo deseamos, una clave de cifrado para el archivo de copia. Como en cada paso que implique cierto tiempo, es recomendable realizarlas estando seguros que el proceso no será interrumpido por motivos ajenos a la tarea.

- Restaurando copia de seguridad

$ adb restore Android.ab

De nuevo, en el dispositivo nos aparecerá una pantalla de confirmación para la restauración y, en su caso, nos pedirá la clave de cifrado con la que se realizó la copia de seguridad.

4.2.3 Copias de seguridad/sincronización vía Google



Por último, vamos a ver cómo realizar una copia de seguridad usando a un tercero, en este caso Google. Aunque existen infinidad de programas y servicios que nos ayudarán a realizar estas copias, sin duda Google es la forma más extendida y más integrada en el sistema. Esta opción no está recomendada en el entorno corporativo, salvo que esté permitida por la política de su organización.

Para realizar este paso es necesario disponer de un terminal móvil asociado a una cuenta de Google. Esto es muy común, ya que es uno de los primeros pasos a realizar la primera vez que se configura el dispositivo. Para realizar una copia nos dirigiremos a Ajustes → Copia de seguridad. Una vez en este punto, simplemente activaremos la opción "Copia mis datos". De esta forma tendremos una forma automática de realizar copias de seguridad de nuestros datos, aplicaciones y claves, y que además es configurable en las opciones de nuestra cuenta. De tal forma que, siempre que tengamos configurada nuestra cuenta de Google en el dispositivo, podemos sincronizar la información almacenada en éste con la de nuestra cuenta (almacenada en los servidores de Google).

5 PERMISOS EN APLICACIONES

Otro de los puntos críticos a tener en cuenta desde el punto de vista de la seguridad, son las aplicaciones y, más concretamente, sus permisos. Los permisos de las aplicaciones son las capacidades, libertades de acceso a archivos o funcionalidades del sistema que las aplicaciones necesitan, o al menos solicitan, antes de ser instaladas. En el año 2014 el market oficial "Google Play" realizó un cambio en el modelo de permisos buscando un sistema simplificado/agrupado, de tal forma que todos los permisos de Android han quedado reducidos, de aproximadamente unos 150 permisos a unos 12 grupos (Ver anexo). Así que, al aceptar otorgar permisos a una aplicación para uno de estos grupos, estamos aceptando todos los permisos que lo componen. Aparte de estos permisos, debemos tener en cuenta que aunque las aplicaciones no lo indiquen, todas tienen permiso por defecto para usar nuestra conexión a internet.

Si somos usuarios de Android, ya sabremos que si queremos instalar una aplicación, debemos aceptar todos los permisos que esta solicite. No podemos elegir cuáles aceptamos y cuáles no. Así que

debemos ser muy conscientes de qué funcionalidad tiene la aplicación que instalamos y qué permisos nos está pidiendo. ¿Tiene sentido que la app de una calculadora tenga acceso a nuestros contactos o a nuestra posición mediante geolocalización? Es obvio que no. Por tanto, deberíamos concienciarnos que en muchos casos deberíamos preguntarnos si realmente necesitamos esa aplicación que quizás esté pidiendo

permisos que no queramos otorgar. Siempre podremos buscar otra aplicación con una funcionalidad parecida cuyos permisos estén más acorde con las acciones que realiza.

6 OTRAS CONFIGURACIONES DE SEGURIDAD

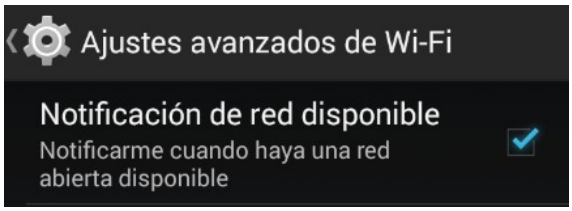
Aparte de la protección frente accesos físicos y el control de las acciones que permitimos que las aplicaciones instaladas realicen en nuestro dispositivo, tenemos otros puntos vulnerables que debemos fortificar.

6.1 Conectividad

Dentro de las posibilidades de fortificación de conectividad las más importantes son la conexión Wi-Fi y Bluetooth. En cualquier caso, como medida de seguridad se recomienda utilizar el APN corporativo en la conexión de datos móviles.

6.1.1 WIFI

El mejor consejo para mantener cierta seguridad en la conectividad de nuestro dispositivo a través de redes wifi, es que no activemos la interfaz de red wifi del dispositivo salvo que queramos conectarnos de forma consciente. Además, debemos conectarnos únicamente a redes conocidas y de confianza. Esto quiere decir que mantengamos todo el tiempo la capacidad wifi del terminal apagada y que sólo nos conectemos a redes conocidas, evitando las típicas redes “libres”. Para ello hay alguna configuración que nos ayudará a que nuestro terminal no se conecte a ciertas redes. En el menú Ajustes → Wi-Fi → Ajustes avanzados, podemos desactivar la opción “Notificación de red disponible”. Esto evitará que las notificaciones nos indiquen la existencia de redes abiertas disponibles.

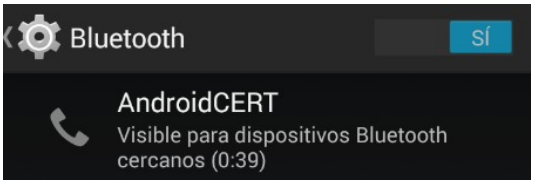


Un detalle a tener en cuenta es saber que el estado de la interfaz wifi se mantiene cuando el terminal es reiniciado, por lo que debemos tener presente que si ésta estaba encendida, al reiniciar el terminal la interfaz de red wifi seguirá encendida.

6.1.2 Bluetooth

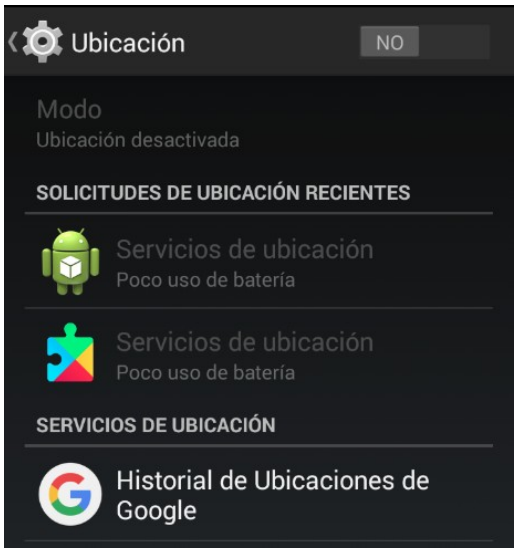
Al igual que en el caso de la wifi, la mejor recomendación de seguridad es no tener activada esta interfaz a menos que sepamos que vamos a hacer un uso de ella. Evitando de esta forma la interacción malintencionada de terceros con nuestro dispositivo mediante esta vía de comunicación. De nuevo, y al igual que pasaba con la interfaz wifi, hay que tener en cuenta que ésta mantiene su estado tras un reinicio del dispositivo.

Dentro de Ajustes → Bluetooth → Ajustes avanzados, disponemos de ciertas configuraciones de seguridad. Además de encender o apagar la interfaz, podemos permitir que nuestro dispositivo no se anuncie a terceros, eligiendo entre las opciones "oculto" o "visible". También podemos definir el nombre con el que identificaremos el terminal vía Bluetooth. Existe un modo intermedio entre oculto y visible, se trata de un temporizador llamado "Tiempo de visibilidad", que nos permitirá que nuestro terminal se anuncie el tiempo necesario para realizar una asociación con otro dispositivo y, tras esto, dejará de ser visible una vez transcurrido el tiempo indicado.



6.2 Localización GPS

El sistema principal de localización de Android es el GPS (Global Positioning System) pero hay que tener en cuenta que no es el único. Mediante las conexiones wifi que realizamos Google es capaz de geolocalizarnos, aunque con algo menos de precisión que vía GPS. No obstante, debemos comprender que nuestra situación geográfica, para bien o para mal, es conocida. Aunque apaguemos el GPS y la interfaz wifi, siempre podremos ser ubicados por la triangulación de las antenas de la red de telefonía móvil. Por tanto, si no quisiéramos ser localizados, la única forma es mediante el estado llamado "modo avión".

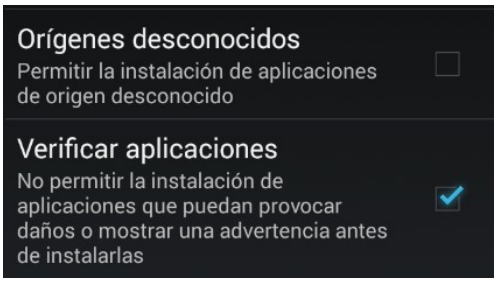


En cualquier caso, es interesante ser consciente de cuáles de las aplicaciones que corren en el dispositivo hacen uso de nuestra localización. Esto puede lograrse accediendo a Ajustes → Ubicación. Dentro de esta pantalla veremos las "Solicitudes de ubicación recientes" y los "Servicios de ubicación". Este sitio puede resultar útil para conocer si hemos instalado alguna aplicación que accede a nuestra localización y que no queríamos que lo hiciera.

En la imagen de esta sección podemos ver el servicio "Historial de Ubicaciones de Google", donde se observa que la empresa californiana guarda un registro de nuestras ubicaciones. Esto puede ser un gran fallo de seguridad si alguien accede física o lógicamente al terminal, puesto que el intruso podría saber cuáles son nuestras localizaciones habituales. Esta funcionalidad puede, y debería ser, deshabilitada siempre que no sea necesaria para ciertas aplicaciones de Google que queramos usar.

6.3 Comprobación de seguridad de las aplicaciones

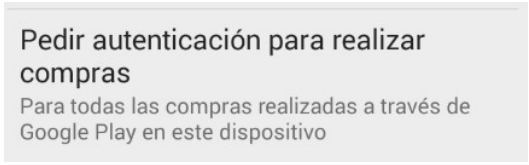
Los dispositivos Android están ampliamente expuestos a la instalación/ejecución de aplicaciones con malware o modificadas. Muchas veces instaladas desde el market oficial, Google Play. Ante este peligro los dispositivos Android poseen ciertas capacidades que les permiten comprobar las aplicaciones antes de ser instaladas e incluso las versiones más modernas pueden comprobar las aplicaciones después de haber sido instaladas. Android, mediante el uso del servicio Google Bouncer, puede avisarnos del peligro al instalar una aplicación no verificada o catalogada como maliciosa, incluso cuando no se instalan desde Google Play. Este servicio compara la aplicación con la base de datos que posee y avisará al usuario si la app es dañina, llegando incluso a no permitir su instalación.



Dentro de la sección Ajustes → Seguridad, tenemos la opción "Verificar aplicaciones". Esta es la que debemos tener activada para que Google pueda comprobar la aplicación que vamos a instalar. En los modelos más recientes, también comprobará aplicaciones instaladas previamente y que se ha descubierto que son maliciosas. Para forzar más la seguridad, incluso podemos impedir la instalación de aplicaciones desde "Orígenes desconocidos".

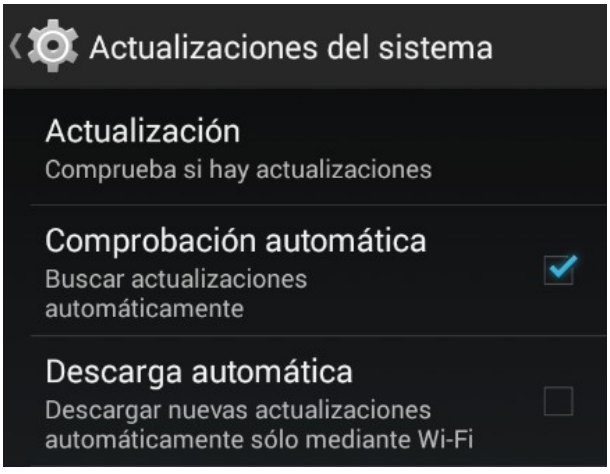
6.4 Compras indeseadas

Cada vez es más habitual la realización de compras/transacciones económicas a través de nuestro terminal. Para poder realizar estas compras normalmente es necesario tener dado de alta un método de pago como Paypal, tarjeta de crédito o mediante el uso de códigos. Métodos como Paypal tienen su propia seguridad mediante la autorización en portal seguro y código de acceso... Android te proporciona un método adicional de seguridad vinculado a tu cuenta de Gmail. Dentro de la aplicación Google Play → Ajustes, podemos encontrar la opción "Pedir autenticación para realizar compras" Esta opción es muy útil ante la realización de compras accidentales o maliciosas, puesto que antes de realizar cualquier compra, el sistema nos pedirá una confirmación mediante la introducción de las credenciales de la cuenta de Gmail asociada.



7 ACTUALIZACIÓN SISTEMA OPERATIVO

En Android, como en cualquier otro sistema operativo, es importante mantener las aplicaciones y el propio sistema actualizados. Este es un punto esencial para la defensa contra atacantes que aprovechan agujeros de seguridad para vulnerar el sistema y acceder a nuestros datos. Para ello, podemos comprobar si existen nuevas versiones de software pidiendo a Android que, de forma automática, realice estas comprobaciones. Obviamente, también es posible realizar una comprobación manual. En el menú Ajustes → Información del teléfono → Actualización del sistema, podemos configurar que el terminal nos avise cuando se publique una nueva versión de Android marcando la opción "Comprobación automática". También podemos forzar el proceso pulsando sobre la opción "Actualización".



Debemos tener en cuenta, como ya se ha indicado en otros puntos de este documento, que cualquier proceso pesado como una actualización del sistema debe ser tomado en consideración e intentar realizarlo sólo cuando podamos garantizar la conexión y la alimentación del dispositivo.

En relación al tema de la actualización del sistema operativo, existen ciertas peculiaridades que diferencian a Android de la mayoría de sistemas operativos que los usuarios están acostumbrados a usar. La principal diferencia es la falta de compromiso de los fabricantes de los terminales en lanzar actualizaciones de forma periódica, produciéndose en muchos casos la paradoja de que habiéndose publicado una actualización de Android que corrige graves deficiencias de seguridad del sistema, esta actualización tarde muchos meses en llegar al usuario final o ni siquiera llegue. Esto nos puede dar una idea de la gran cantidad de sistemas Android vulnerables que existen en circulación. La complejidad y la

falta de acuerdo entre los diferentes fabricantes, Google y las versiones distribuidas por las operadoras de telefonía, mantiene a la mayoría de usuarios de Android indefensos ante gran cantidad de ataques ya conocidos.

Además de la tardanza en el lanzamiento de las actualizaciones en las versiones del sistema operativo, también es frecuente la "obsolescencia programada" por el propio fabricante.

8 ANTIVIRUS

Una de las lacras del mundo tecnológico son los programas realizados con fines ilegítimos o malintencionados (el popularmente conocido malware). Como una plaga, hoy en día se generan miles de estos programas al día. Tanto es así que se considera que hay más terminales que están o han estado infectados que los que que nunca han sido comprometidos. A fin de luchar contra estos programas existen distintas soluciones, pero sin duda la mas habitual, extendida y amigable para el usuario, es el "Antivirus". Es recomendable el uso de uno de estos sistemas antimalware en cada terminal. Pero estos programas no son perfectos, por ello a la hora de elegir qué antivirus debemos instalar podemos tener en cuenta los siguientes puntos:

- **Herramientas del tipo corporativo:** Generalmente los principales fabricantes de seguridad TI ofrecen dos gamas de sus herramientas: las versiones para usuarios domésticos y las enfocadas a un entorno corporativo. Por supuesto, si su organismo le proporciona un Antivirus corporativo, úselo.
- **Diversidad de catálogo:** Se debe considerar que probablemente en un futuro, y dependiendo de las necesidades de la organización, se requiera añadir más herramientas de seguridad que complementen a la aplicación antivirus primaria con la que se debería contar. El fabricante que se escoja debería tener un catálogo amplio de herramientas y aplicaciones disponibles que cubran futuros requerimientos complementarios, como antispam, backup y restauración, etc.
- **Actualizaciones de firmas:** Elegir un sistema que actualice sus firmas de reconocimiento de malware de forma rápida y fácil para su actualización en el terminal.
- **Facilidad de uso:** Siempre que sea posible hay que probar estos antivirus; no todos son fáciles de configurar y usar. Muchos de ellos pueden hacer difícil el uso del terminal.
- **Gasto extra de batería:** Muchos de estos antivirus/antimalware producen un gasto excesivo de batería.

Pero sin duda la mejor característica que debe poseer un antivirus es el que es capaz de detectar/eliminar la mayor cantidad de malware posible.

9 CONCLUSIONES

Nuestros terminales son portales a nuestras casas, familiares, amigos y trabajo. Debemos ser conscientes de que al protegernos, también lo hacemos con las personas que nos rodean. Ninguna de las configuraciones que hemos propuesto en este documento nos ofrecen una protección al 100%, aunque la combinación de las diferentes técnicas expuestas nos garantizará un grado de seguridad razonablemente

aceptable.. La mejor protección es un usuario consciente de los riesgos y dispuesto a tomas las decisiones necesarias en pro de su seguridad, aunque estas decisiones conlleven, sobre todo al principio, cierto esfuerzo por su parte.

En el entorno corporativo se recomienda el uso de una plataforma de gestión de dispositivos móviles (MDM – Mobile Device Management) para la gestión centralizada de los dispositivos móviles [6].

10 ANEXO

10.1 Lista simplificada de permisos Android

- **Servicios por los que tienes que pagar** – llamar directamente a números de teléfono (de moderada a gran relevancia).
- **Servicios por los que tienes que pagar** – envío SMS/MMS (de moderada a gran relevancia).
- **Almacenamiento** – modificar/borrar archivos en la tarjeta SD (gran relevancia). Permites la lectura de archivos y su eventual modificación, típico en apps de backup.
- **Tu información personal** - leer datos de contacto (gran relevancia). Lejos de las que piden este permiso por un motivo lógico, como las apps que utilizan la agenda para el envío de mensajes, hay que replantearse si proporcionar este permiso a otro tipo de aplicaciones.
- **Tu información personal** - leer datos de calendario, modificar datos de calendario (de moderada a gran relevancia). Por los mismas razones que el caso anterior, hay que considerar detenidamente si una app nos pide este permiso con sentido o no.
- **Llamadas de teléfono** – leer estado del teléfono e identidad (de moderada a gran relevancia). Hay que tener cuidado con este permiso, porque si bien es normal que muchas apps te lo pidan para funcionar mientras hablas, a la vez permite el acceso a tu IMEI, IMSI y al identificador único de 64 bits que Google asigna a cada terminal, con todo lo que ello podría conllevar.
- **Tu ubicación** – precisar la ubicación (GPS) (moderada relevancia). Al fin y al cabo localiza nuestra posición.
- **Tu ubicación** – ubicación común (basada en red). De igual manera, te localiza por tu conexión a la red. Es menos precisa que la geolocalización por GPS.
- **Comunicación de red crear conexión Bluetooth** (baja relevancia).
- **Comunicación de red** – ver estado de conexión, ver estado de Wi-Fi (baja relevancia). Sólo se fija en tu estado.
- **Herramientas del sistema** – Impedir que el teléfono entre en modo de suspensión (baja relevancia). Son escasos los tipos de aplicación que pueden necesitar de este permiso, y realmente a lo único que puede afectar es a nuestra batería, pero es necesario. GPS, e-readers ...
- **Herramientas del sistema** – Modificar la configuración global del sistema (moderada relevancia).

- **Herramientas del sistema** – leer ajustes de sincronización (baja relevancia). Tan sólo permite saber si tienes sincronización en segundo plano con alguna aplicación (como un cliente de Twitter o Gmail).
- **Herramientas del sistema** – escribir configuración del Punto de Acceso (moderada relevancia). Relativa a la configuración global. En principio se refiere a encender y apagar tu conexión de red o Wi-Fi.
- **Herramientas del sistema** – reiniciar automáticamente al encender (de baja a moderada relevancia). Como es de suponer, consiste en que la aplicación se inicie nada más encender el teléfono.
- **Herramientas del sistema** – reiniciar otras aplicaciones (de baja a moderada relevancia).
- **Herramientas del sistema** – recuperar aplicaciones en ejecución (moderada relevancia). Permite saber qué aplicaciones están corriendo en segundo plano.
- **Herramientas del sistema** – establecer aplicaciones preferidas (moderada relevancia). Permite la asignación a una aplicación para que haga determinada tarea de una cierta manera, por ejemplo, con un cliente como Twitter cuando asignamos una aplicación concreta para el visionado de enlaces o imágenes.
- **Controles de hardware** – control de la vibración (baja relevancia).
- **Controles de hardware** – realizar fotografías (baja relevancia) .
- **Controles de hardware** – realizar vídeos (baja relevancia).

11 DOCUMENTACION DE REFERENCIA

[1] Microsoft Word - Guia uso seguro de Android.doc - [CSIRTcv] Guia uso seguro de Android.pdf

[2] Conoce los Permisos de Seguridad en Android - El Androide Libre

[3] Guía seguridad android eset.pdf

[4] Guía de seguridad Android CCN-CERT

[5] Realizar una copia de seguridad completa de un dispositivo Android

[6] Gestión de dipositivos móviles de RCJA