CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

USO SEGURO DE ANDROID

Documento Público

Marzo 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. Uso seguro de dispositivos Android....4
2. Introducción....4
3. Seguridad de la información....5
   3.1. Pantalla de bloqueo....5
   3.2. Personalizar mensaje en la pantalla de bloqueo....8
   3.3. Información médica de emergencia....8
   3.4. Definir los contactos de emergencia....10
   3.5. Cifrado de la información....11
   3.6. Copias de seguridad....12
   3.7. ¿Memoria interna o Tarjeta SD?....13
4. ¿Qué son los permisos y cómo funcionan?....14
5. Configuración segura....17
   5.1. Wifi....17
   5.2. Bluetooth....17
   5.3. NFC....18
   5.4. Privacidad / Localización....19
   5.5. Buscar mi dispositivo Android, bloquearlo o borrarlo....19
   5.6. Análisis de aplicaciones sospechosas....20
   5.7. Acceso a notificaciones....21
6. Actualizaciones del sistema operativo y de las aplicaciones....21
7. Instalación desde fuera de Google Play....23
8. Evitar compras en aplicaciones....24
9. Instalar teclados alternativos....25
10. ¿Antivirus en el móvil?....25
11. Contacto y consultas....27

1. Uso seguro de dispositivos Android

La presente guía explica los principales aspectos a tener en cuenta para utilizar un dispositivo Android de forma segura: configuración ideal, instalación segura de aplicaciones, protección de la información y de las comunicaciones. Quedan para otro momento temas avanzados como las implicaciones de hacer "root" a un dispositivo, cómo limitar los permisos de las aplicaciones o las ventajas y riesgos de instalar "roms" alternativas.

2. Introducción

Android es un sistema operativo basado en Linux y diseñado inicialmente para dispositivos móviles. Google lo presentó en 2007 y desde entonces ha crecido imparable hasta llegar a hacerse con una cuota de mercado cercana al 90%.

Debido a la progresiva expansión que ha tenido Android entre usuarios "poco tecnológicos", no siempre se es consciente de los riesgos derivados de utilizar este tipo de dispositivos: están expuestos a peligros similares a los de los ordenadores, tienen conectividad con Internet, se utilizan para almacenar información personal como fotografías o vídeos, se utilizan para acceder a nuestra vida online como redes sociales, correo o banca electrónica, pueden infectarse con virus informáticos o ser fácilmente robados o perdidos.

Para hacer frente a la falta de formación y concienciación existente, en esta guía se explicarán todas aquellas cuestiones relativas a la seguridad de los dispositivos, sus comunicaciones y la información que almacenan.

Se debe destacar que existen multitud de versiones de Android: las primeras versiones que llegaron masivamente al gran público fueron las 2.x, de las cuales aún quedan dispositivos funcionando. Paralelamente aparecieron las 3.x destinadas a las tabletas electrónicas, para seguir evolucionando en las sucesivas versiones que siguen apareciendo.

Dependiendo de la versión de Android, podría haber alguna pequeña diferencia en los pasos que vamos a detallar para acceder a los diferentes ajustes que nos ayudarán a mejorar la seguridad del dispositivo.

3. Seguridad de la información

Generalmente no somos conscientes de la cantidad de información que almacenamos en nuestros teléfonos móviles.

Si nos preguntan acerca de la información que contienen nuestros dispositivos, seguramente diremos que algunas fotos y algún correo, pero la realidad es bien distinta hasta el punto de que si toda la información que contiene cayese en malas manos podría causarnos un daño importante.

Para hacernos una idea podemos plantearnos el peor de los casos en el que alguien con muy malas intenciones nos robase el móvil:

• Podría leer nuestras últimas conversaciones de chat como pueden ser WhatsApp o Hangouts y suplantar nuestra identidad insultando o enviando contenidos inapropiados a familiares, parejas, amigos o incluso jefes.

• Podría acceder a nuestras redes sociales y de nuevo causar estragos entre nuestros amigos, cambiar la configuración de privacidad para que todos los usuarios puedan ver todo, o incluso borrarnos la cuenta.

• Podría copiar toda nuestra lista de contactos y publicarla en Internet con el único fin de dañar también a nuestros amigos. Imaginemos esta situación si además tenemos apuntada la dirección postal de los mismos o direcciones de clientes.

• Podría acceder a nuestro historial de navegación web, historial de búsquedas, de ubicaciones, o de aplicaciones, donde se podría encontrar contenido comprometido.

• Podría publicar cualquier tipo de fotografía o vídeo que tengamos en el móvil, compartirlo en redes sociales, o enviárselo a todos nuestros contactos mediante mensajería instantánea.

• Si tenemos configurada alguna aplicación de compras online, como la de Amazon o el propio Google Play, podría comprar artículos a cargo de nuestra cuenta bancaria.

Por todos estos motivos resulta tremendamente necesario proteger tanto el acceso a nuestro dispositivo móvil, como la información que contiene.

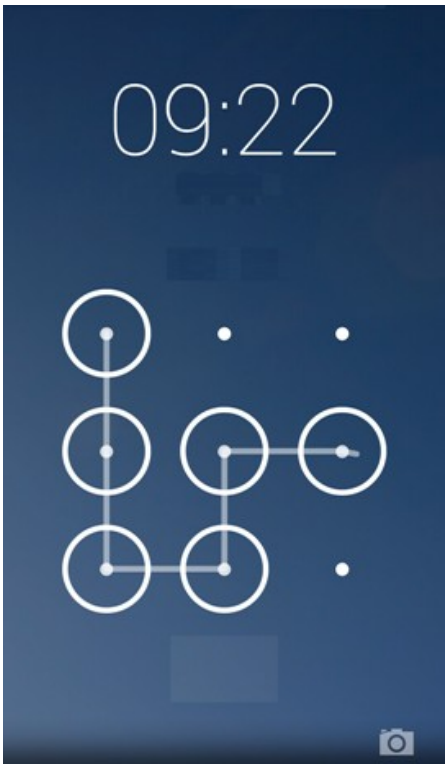
3.1. Pantalla de bloqueo

La primera medida de seguridad imprescindible que hay que activar al recibir un dispositivo con Android es el bloqueo de pantalla. Se trata de hacer que al encender la pantalla del dispositivo, se solicite algún tipo de código o contraseña para poder utilizar el terminal y que si la introducimos mal varias veces haya que esperar un corto periodo de tiempo antes de poder volver a hacer un nuevo intento.

Muchos usuarios se quejan al principio de que no es práctico y de que les quita mucho

tiempo, pero al segundo día esta operación se hace tan instintivamente que todo el mundo acaba acostumbrándose.

Ejemplo de patrón de bloqueo:



Para establecer un método de desbloqueo Android nos ofrece múltiples posibilidades: podemos elegir un PIN, un patrón de desbloqueo (un dibujo), una contraseña, o incluso es posible desbloquear el dispositivo mediante huella dactilar o reconocimiento facial.

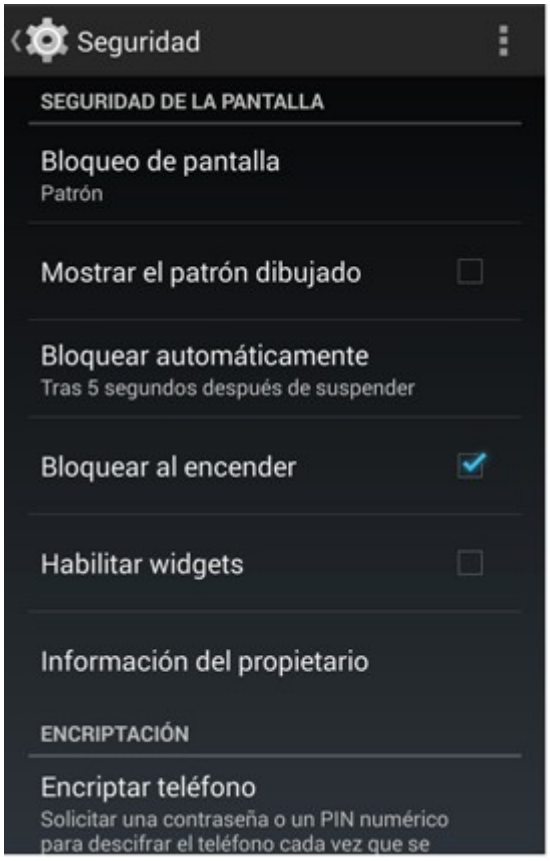
Al configurar este tipo de bloqueo muchos usuarios se preguntan qué sucede si olvidan dicho patrón. En este caso es posible restaurarlo mediante el usuario y contraseña de la cuenta de correo electrónico, o en última instancia mediante el restaurado de fábrica del dispositivo perdiendo todos los datos y configuraciones.

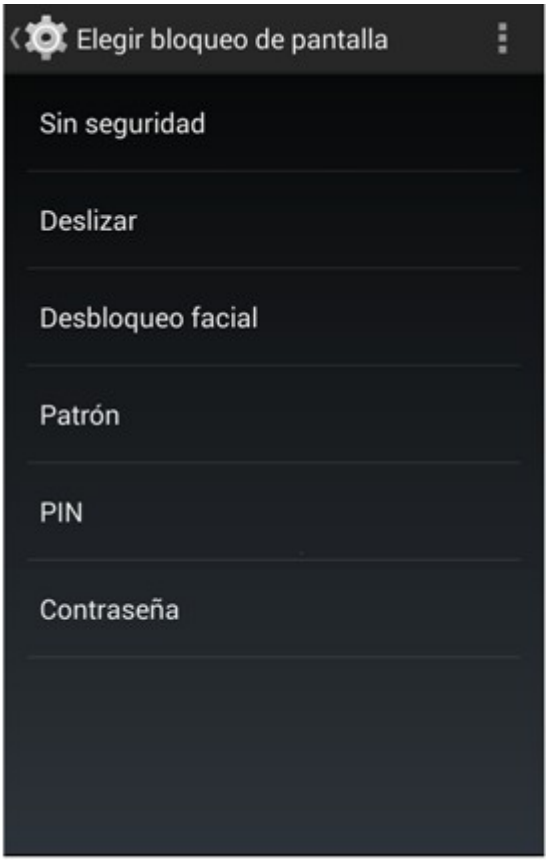
Si bien el restaurado de fábrica puede parecer desproporcionado para algunos usuarios, más adelante veremos cómo hacer copias de seguridad de toda nuestra información para que en caso de pérdida, robo, o restaurado del terminal, no se pierda la información. Además de esta forma garantizamos que si nuestro dispositivo se pierde, lo más común es que el "nuevo dueño" restaure de fábrica el dispositivo para poder utilizarlo, proceso en el cual toda nuestra información se eliminará y no se verá comprometida.

La opción de bloqueo de pantalla se encuentra disponible en las opciones de
Ajustes -> Pantalla bloqueo y seguridad -> Tipo de bloqueo de pantalla.

Además desde “Ajustes del bloqueo seguridad” podremos establecer cuánto tiempo debe pasar para que el terminal se bloquee automáticamente (tiempos de entre 30 segundos y un minuto son adecuados).

Configuración del bloqueo de pantalla:





En caso de utilizar el patrón de desbloqueo, opción más utilizada, será conveniente desmarcar la casilla "Mostrar el patrón dibujado" para protegernos de miradas indiscretas a la hora de dibujar nuestro patrón.

3.2. Personalizar mensaje en la pantalla de bloqueo

Como hemos comentado anteriormente, debemos establecer un bloqueo de pantalla que garantice que nadie pueda tener acceso a utilizar nuestro dispositivo.

Pero en caso de pérdida del teléfono o en caso de emergencia, nadie podrá acceder a nuestros contactos para avisar de la situación. Por tanto, **debemos configurar un texto informativo que aparecerá en pantalla cuando el teléfono está bloqueado y que indicará un número de teléfono al que podrían llamar**.

Para personalizar ese texto, debemos acceder a:
Ajustes > Pantalla de bloqueo > Firma de Pantalla de bloqueo

Es posible que, según el dispositivo, las opciones sean las siguientes:
Ajustes > Pantalla bloqueo y seguridad > Información y accesos directos > Información propietario

Por ejemplo, podemos escribir el siguiente texto:
"(escribir un teléfono al que deberán llamar) para emergencias"

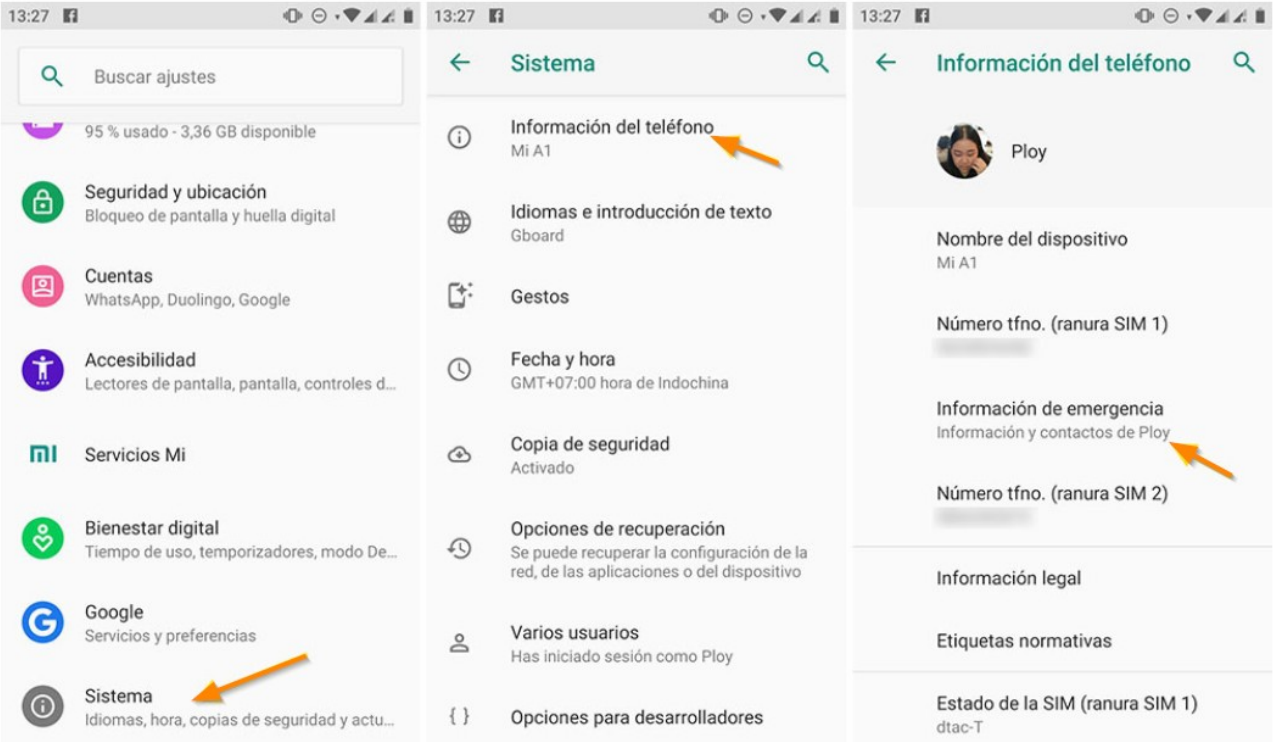
3.3. Información médica de emergencia

En caso de accidente, resulta muy útil tener configurado en el móvil aquella información médica que cualquiera podría ver sin necesidad de desbloquearlo. Pese a que los datos de salud son considerados como datos personales de categoría sensible, sería importante informar del grupo sanguíneo que somos, nuestro peso, la medicación actual, alergias, la fecha de nacimiento para que sepan nuestra edad…

Esta información puede consultarse aunque el móvil esté bloqueado.

Para configurarlo debemos seguir estos pasos:

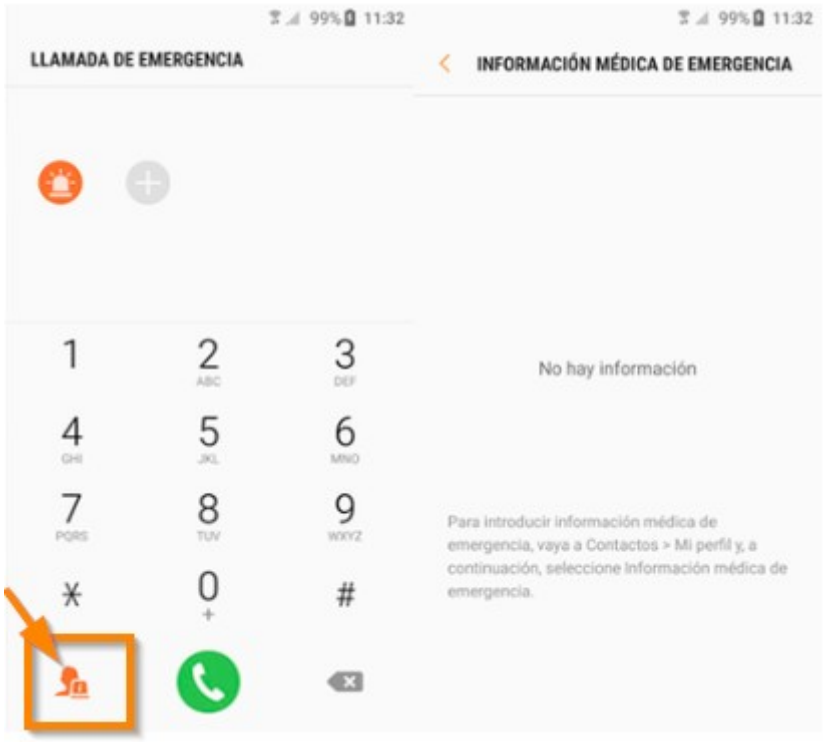
Ajustes > Sistema > Información del teléfono > Información de emergencia > Editar información



Si no te aparecen estas opciones en tu versión de Android, te recomendamos que utilices el buscador que hay en Ajustes para buscar "emergencia" y así ver qué opciones te ofrece tu modelo de dispositivo.

En algunos casos los pasos pueden ser los siguientes:
Acceder a la aplicación Contactos > Mi perfil > Información médica de emergencia

Para ver esta información desde la pantalla bloqueada, presionamos en "Llamada de emergencia" o "Información de emergencia". Según versiones de Android, nos mostrará ya la información o debemos fijarnos en la esquina inferior izquierda, si hay un icono con una silueta de persona, que nos mostrará los datos médicos introducidos.



Dependiendo del fabricante (Samsung, Huawei, BQ, Sony, Xiaomi, etc.) puede variar la apariencia y la forma de acceder a dicha información.

En caso de que el dispositivo no disponga de esta función, podemos instalar alguna aplicación de las que existen en Google Play Store, por ejemplo, Medical ID.

3.4. Definir los contactos de emergencia

Aunque tengamos el teléfono bloqueado, siempre es posible llamar al 112, pero también podemos configurar unos contactos a los que podrían avisar en caso de necesidad.

Para ello debemos introducirlos desde la pantalla de información de emergencia, la misma que hemos explicado en el apartado anterior. Si no localizamos la opción, podemos utilizar el buscador disponible en Ajustes.

En caso de que el dispositivo no disponga de esta función, podemos instalar alguna aplicación de las que existen en Google Play Store, por ejemplo, ICE.

3.5. Cifrado de la información

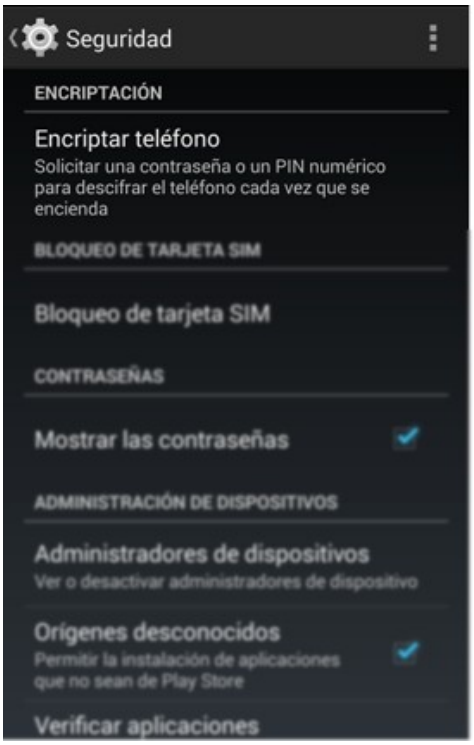
A partir de Android Q todos los dispositivos cifrarán los datos de los usuarios, sin excepciones, siendo esta la configuración por defecto.

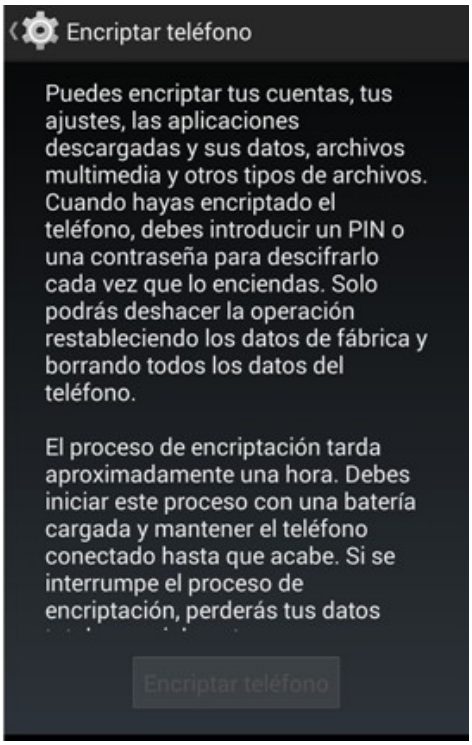
Pero en las **versiones anteriores** de Android, debemos ser nosotros quienes **decidamos si queremos aplicar el cifrado** de los datos.

Tal como hemos visto en el apartado anterior, ante la pérdida o robo de un dispositivo lo más normal es que, si éste tiene bloqueo de pantalla, sea restaurado de fábrica por lo que nuestra información no será accesible por nadie.

No obstante, dependiendo de lo crítica o sensible que sea la información que se almacena en el dispositivo, puede ser que el usuario desee añadir una capa adicional de seguridad por si se consigue averiguar el patrón de bloqueo o el PIN (en ocasiones es posible ver el patrón de bloqueo por las huellas de la pantalla, o engañar al desbloqueo facial con una foto del propietario), o se almacena información en una tarjeta SD (la cual no se borraría en caso de restauración del dispositivo). La Tarjeta SD es una tarjeta de memoria que permite ampliar la capacidad de almacenamiento de algunos dispositivos móviles (no todos tienen esta posibilidad).

Opciones de cifrado:





Pues bien, este nivel extra de seguridad nos lo proporciona el cifrado. Mediante esta técnica se codifica toda la información del antes de acceder a ella, además de ser un proceso irreversible: una vez cifrado el terminal, no es posible volver a dejarlo como estaba salvo que se restaure de fábrica.

Cabe destacar que al aplicar esta configuración, el rendimiento del dispositivo se puede ver reducido.

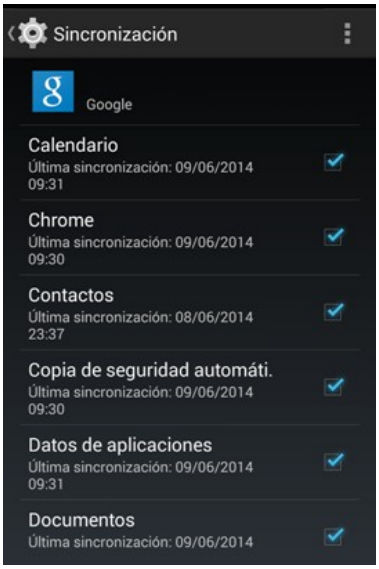
3.6. Copias de seguridad

Hasta el momento hemos hablado de cómo proteger la información de nuestro terminal para que nadie pueda verla sin nuestro permiso, pero también es importante protegerla de que no se pierda junto con el dispositivo o que no se borre sin querer, para lo cual deberemos hacer copias de seguridad.

Android dispone de un pequeño sistema de copias de seguridad que se encarga de copiar aspectos como la configuración del terminal, el listado de aplicaciones instaladas, o la configuración de las redes Wifi de forma que si restauramos el dispositivo de fábrica, una vez introduzcamos nuestra cuenta de Google, todos estos datos empezarán a restaurarse.

Para **crear manualmente una copia de seguridad de los datos y los ajustes**, debemos seguir los siguientes pasos:
Ajustes > Sistema > Copia de seguridad > Crear una copia de seguridad ahora > Continuar.

Este sistema de copias se ve complementado con los diferentes servicios web de que dispone Google y que almacenan online la información que manejamos en nuestros dispositivos móviles. Así pues, si utilizamos los contactos de Gmail (que es el servicio de correo electrónico de Google), al restaurar la configuración de nuestro dispositivo, empezará la sincronización de los contactos de forma que se puede decir que en cierta manera se ha restaurado una copia de seguridad.



Estas copias de seguridad abarcan, entre otros, los siguientes datos:

- Eventos de Google Calendar
- Fotografías y vídeos
- Partidas de juegos integrados con Google Play
- Favoritos del navegador Chrome
- Datos de aplicaciones
- Documentos ofimáticos de Google Drive
- Notas de Google Keep
- Música de Google Music
- Películas de Google Play Movies
- Libros de Google Play Books

Mediante el uso de todas estas herramientas es posible hacer una copia íntegra de todas las aplicaciones que dependen de Google, siendo posible incluso subir el resto de documentos o archivos a Google Drive (que es el servicio de Google de almacenamiento online) para disponer de una copia de los mismos.

3.7. ¿Memoria interna o Tarjeta SD?

Existen móviles que permiten insertar tarjetas de memoria para ampliar capacidad de almacenamiento. Si bien es una práctica muy extendida, no todos los usuarios se plantean cual es el lugar idóneo para guardar su información ni las implicaciones de seguridad que esto puede tener.

Como ya hemos explicado anteriormente, todo dispositivo Android debe tener un código de desbloqueo para evitar que si se pierde o roba el terminal sea posible acceder a la información que contiene. No obstante, si la información se almacena en una tarjeta extraible, sacar la información es tan sencillo como sacar la tarjeta y conectarla a otro dispositivo u ordenador.

Para evitar que información sensible como documentos o fotografías caigan en las manos equivocadas, es recomendable utilizar la memoria externa únicamente para el material que no pueda comprometernos, como pueden ser películas o música, y dejar el espacio de la memoria interna del dispositivo para almacenar nuestras fotografías, vídeos propios o documentos.

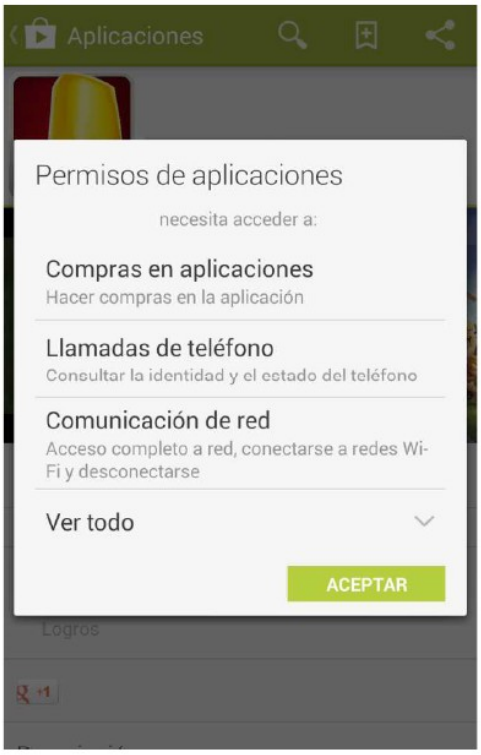
Recordemos que también es posible cifrar la tarjeta externa con las opciones indicadas en apartados anteriores, de forma que aunque se conecte la tarjeta a un PC no será posible acceder a la información.

4. ¿Qué son los permisos y cómo funcionan?

Android dispone de un sistema de permisos que se encarga de gestionar qué aplicaciones tienen acceso a qué información o funcionalidades de nuestro dispositivo.

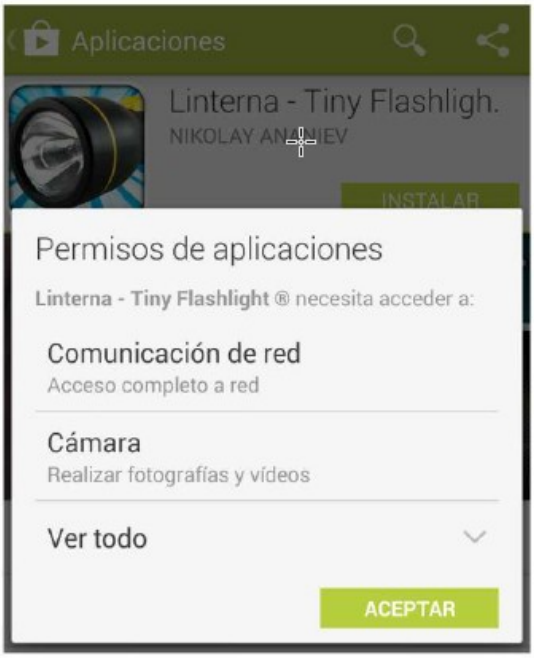
Cuando instalamos una aplicación en nuestro terminal, independientemente de si es desde Google Play o no, siempre se nos informa de qué permisos se le van a conceder y a qué funcionalidades podrá acceder, como pueden ser leer la agenda de contactos, saber la ubicación del terminal, conectar con Internet, o incluso hacer llamadas o enviar SMS.

Ejemplos de permisos que pueden solicitar las aplicaciones:



Resulta extremadamente importante que prestemos mucha atención a los permisos de las aplicaciones, especialmente de aquellas que no vengan de desarrolladores conocidos o páginas web no oficiales, para evitar que la seguridad de nuestra información se vea comprometida o incluso para evitar ser víctima de estafas y engaños.

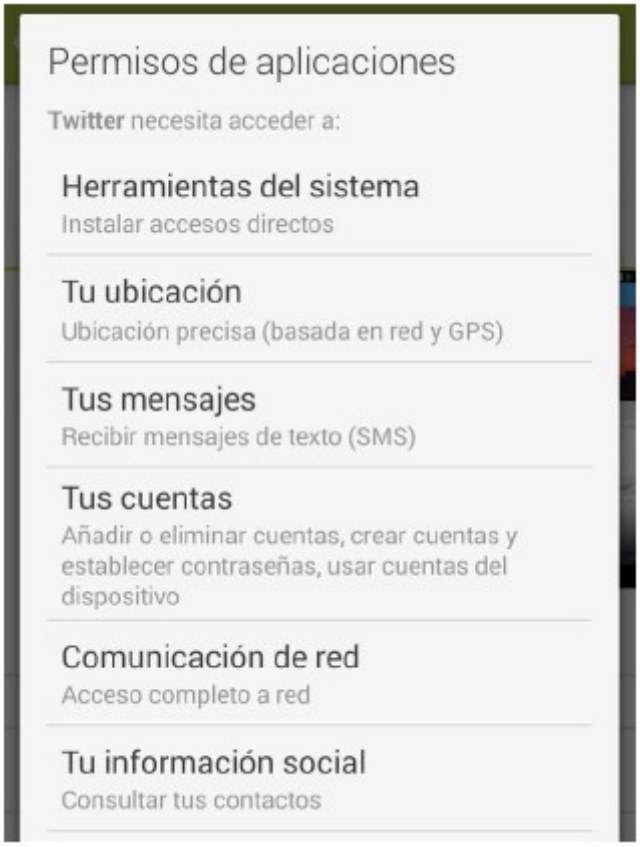
Para ver la importancia de la gestión de permisos hemos tomado dos aplicaciones de Google Play que, en teoría, lo único que hacen es encender el flash de la cámara de fotos para poder utilizar el móvil como linterna.



Si observamos los permisos de ambas aplicaciones, vemos que la de la derecha únicamente necesita acceso a la cámara (para encender el flash) y acceso a Internet posiblemente para enviar estadísticas o buscar actualizaciones. No obstante la de la izquierda solicita tener acceso al GPS, micrófono, otras aplicaciones e incluso a poder hacer compras en aplicaciones. Evidentemente no deberíamos elegir la linterna de la izquierda ya que pide muchísimos más permisos de los que realmente necesita, lo cual puede indicar que se va a hacer un uso fraudulento de la aplicación.

Cabe destacar que la linterna de la derecha pide acceso a Internet, algo que a priori no debería necesitar, pero que al no tener acceso a ninguna otra información de nuestro dispositivo como la galería de imágenes, SMS, contactos, no entraña un riesgo directo.

En este otro ejemplo podemos observar algunos de los permisos de la aplicación Twitter (es una red social muy popular que permite publicar mensajes de hasta 280 caracteres):



- Se solicita permiso para acceder a la ubicación para poder geoposicionar los *twitts*
- Se solicita acceder a los mensajes de texto SMS para poder verificar el número de teléfono
- Se solicita acceder a las cuentas del terminal para poder añadir la cuenta de Twitter
- Se solicita tener acceso a Internet para poder enviar y recibir *twitts*
- Se solicita acceso a los contactos para poder importarlos y buscar contactos en Twitter

Si bien los permisos a "Tus cuentas" y "Comunicación de red" son necesarios para el buen funcionamiento de la aplicación, muchos usuarios pueden pensar que los permisos de acceso a los SMS, la ubicación o a la agenda de contactos son excesivos. Es de esperar que un desarrollador/proveedor reconocido como Twitter no acceda a nuestros contactos ni ubicación para fines diferentes de los propios de la aplicación, pero por desgracia de momento no existe una solución oficial por parte de Android para poder restringir los permisos que no queramos otorgar a las aplicaciones, así que deberemos elegir entre utilizar la aplicación o buscar alguna otra alternativa como puede ser navegar por Twitter solo desde su página web.

5. Configuración segura

Una vez explicadas las principales consideraciones a tener en cuenta para proteger la información almacenada en nuestro dispositivo, se va a dar un repaso por los principales parámetros de configuración que tiene Android, explicando aquellos relevantes para evitar que nuestro terminal se infecte con un virus, que espíen nuestras conversaciones, o incluso para evitar que se hagan pagos con nuestro móvil sin permiso.

5.1. Wifi

Cada vez más usuarios de dispositivos móviles están concienciados de que es altamente peligroso conectarse a redes Wifi desprotegidas (aquellas que no llevan contraseña), ya que por norma general resulta muy sencillo interceptar la información que por ahí se envía, incluyendo conversaciones y contraseñas de acceso.

No obstante, esta no es la única consideración a tener en cuenta en lo que a redes Wifi se refiere: existen una serie de ataques informáticos mediante los cuales por el simple hecho de tener la conexión Wifi activada es posible robar la contraseña de algunas de las redes a las que previamente nos hayamos conectado. Es importante pues, que **mientras no estemos utilizando la conexión Wifi la apaguemos**, ya que además de reducir el consumo de batería conseguiremos mejorar nuestra seguridad.

5.2. Bluetooth

De forma similar a lo que sucede en las conexiones Wifi, existen diferentes ataques informáticos mediante los cuales se puede acceder a información de nuestro teléfono móvil a través del Bluetooth. Por norma general este tipo de ataques intentarán acceder a nuestra agenda de contactos o archivos multimedia (fotos y vídeos), además de intentar utilizar nuestra conexión de datos o incluso realizar llamadas telefónicas.

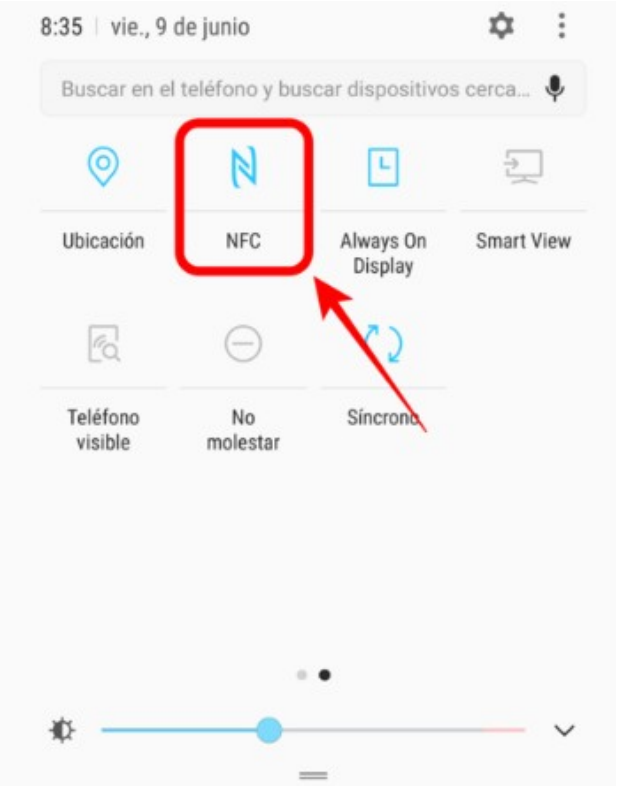
Este tipo de ataques suele aprovechar agujeros de seguridad en los programas que utilizan los fabricantes de los dispositivos móviles, por lo que son diferentes para cada modelo y sistema operativo, de manera que la única forma de proteger nuestros datos es mediante la **desconexión del Bluetooth cuando no lo estemos utilizando**.

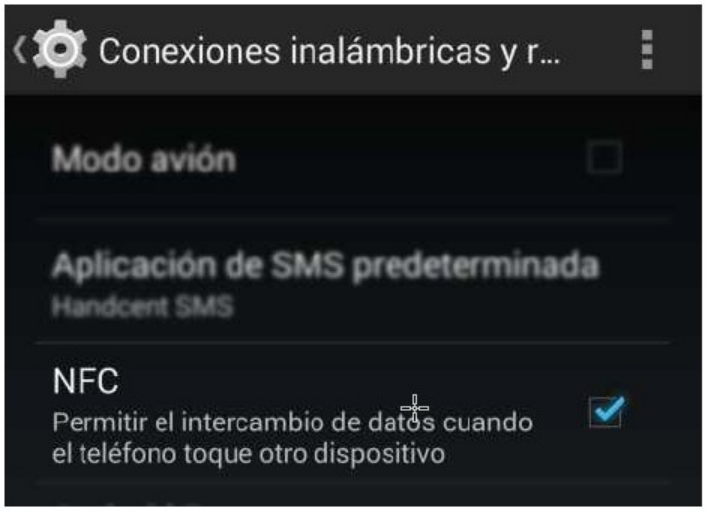
Por otro lado cabe destacar que la mayoría de dispositivos a los que conectamos nuestros terminales por Bluetooth acostumbran a tener una contraseña por defecto que rara vez cambiamos (en ocasiones ni siquiera es posible) por lo que dependiendo del dispositivo (manos libres, otros móviles, electrodomésticos inteligentes, etc.) es posible desde poder controlarlo, hasta acceder a los datos que contenga. En los casos en que sea posible hacerlo, es muy recomendable cambiar la contraseña por defecto que suele ser 0000 ó 1234.

5.3. NFC

La tecnología NFC (Near Field Communication) permite identificar dispositivos y objetos solo con acercarlos a un lector o entre ellos mismos.

De esta forma, si asociamos un dispositivo móvil a una cuenta bancaria o tarjeta de crédito podríamos utilizarlo para pagar de forma similar a como haríamos con la tarjeta. Actualmente se trata de una tecnología robusta que imposibilita el clonado de dispositivos y su falsificación (aunque aún existen en uso versiones antiguas vulnerables), y cuya principal vulnerabilidad es la posibilidad de que llevando nuestro dispositivo/tarjeta NFC en el bolsillo, alguien se aproxime con un lector portátil y haga un pago sin nuestro consentimiento.





Es por ello que los dispositivos móviles que disponen de tecnología NFC requieren que el dispositivo esté desbloqueado para evitar este tipo de situaciones. Pues bien, existen programas que permiten cambiar este comportamiento para que el NFC esté siempre activo y así facilitar la vida al usuario (a cambio de comprometer su seguridad), por lo que **se recomienda** encarecidamente no modificar esta configuración y **requerir siempre que se desbloquee el dispositivo para utilizar el NFC**.

Si no se utiliza esta tecnología, es incluso recomendable desactivarla, y **activarla únicamente cuando sea necesaria para poder hacer un pago**. Esta opción se desactiva desde la barra de notificaciones o desde Ajustes > Conexiones > NFC.

5.4. Privacidad / Localización

La mayoría de dispositivos Android dispone de tecnología GPS que permite conocer la ubicación del terminal y por tanto del usuario. Esta tecnología se utiliza principalmente en aplicaciones de mapas, o aplicaciones de búsqueda para, por ejemplo, ofrecernos resultados de búsqueda cercanos (bares, comercios, etc.). Bien utilizada esta tecnología resulta increíblemente útil, pero existen aplicaciones que hacen uso de ella sin que muchas veces seamos conscientes de ello.

Es el caso de aplicaciones que aparentemente no necesitan utilizar para nada el GPS pero que solicitan acceso al mismo para, por ejemplo, enviar al desarrollador la posición del usuario y averiguar desde qué países o zonas se descarga más su aplicación, o incluso mostrarle publicidad personalizada.

Otras aplicaciones, como las que utilizamos para navegar por redes sociales, sí que pueden necesitar en ocasiones acceso a la ubicación de nuestro GPS para publicar nuestra posición o buscar locales cercanos. No obstante, tras analizar algunas de ellas se ha observado que independientemente de si se desea o no compartir la ubicación, algunas de ellas consultan periódicamente la posición del terminal, comportamiento que nada tiene que ver con acciones realizadas por el usuario.

Si no se desea que estas aplicaciones estén continuamente monitorizando nuestra posición, es suficiente con desactivar las opciones de ubicación de nuestro dispositivo Android desde Ajustes > Conexiones > Ubicación.

Además, desde esta pantalla existe la posibilidad de limitar el acceso a nuestra posición por parte de algunas aplicaciones de Google como pueden ser Google Now o las búsquedas. Si desactivamos los informes de ubicación, las aplicaciones de Google dejarán de utilizar estos datos, y si además desactivamos el "Historial de ubicaciones" se desactivará el histórico de dónde hemos estado, mejorando así nuestra privacidad.

5.5. Buscar mi dispositivo Android, bloquearlo o borrarlo

Para poder localizar un dispositivo Android que has perdido o te han robado, 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, desde otro dispositivo o desde un ordenador:
https://www.google.com/android/find

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 dispositivo**, para que elimine definitivamente todos los datos 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.

5.6. Análisis de aplicaciones sospechosas

Una de las características más criticadas de la seguridad de los dispositivos Android, es que resulta relativamente sencillo instalar accidentalmente aplicaciones fraudulentas, ya sea desde fuentes externas, como en ocasiones desde el propio Google Play. Estas aplicaciones fraudulentas son en ocasiones copias de aplicaciones oficiales y 100% funcionales, pero que al ser descargadas de páginas no oficiales contienen algún tipo de virus, hacen compras en aplicaciones a nuestro cargo o simplemente espían nuestros dispositivos.

Para paliar esta amenaza, Google dispone de un sistema por el cual se verifica automáticamente si alguna de las aplicaciones que tenemos instaladas en el dispositivo es potencialmente sospechosa de ser maliciosa.

Para hacer uso de esta funcionalidad únicamente debemos activarla desde
Ajustes > Google > Seguridad > "Google Play Protect".

Si bien esta funcionalidad no es infalible, es una medida más de seguridad a tener en cuenta.

5.7. Acceso a notificaciones

Existen aplicaciones que piden poder acceder a las notificaciones de nuestro dispositivo para poder operar normalmente. Es el caso de aplicaciones para modificar el icono de la batería o aquellos que deban cambiar el aspecto de la barra de estado.

Aunque este comportamiento no pueda parecernos sospechoso, debemos tener en cuenta que si la aplicación lee todas las notificaciones, también podrá leer parte de nuestras conversaciones o correos electrónicos. Es por ello que Android nos avisará expresamente en caso de que una aplicación intente conseguir permiso para leer las notificaciones del terminal, y solo deberemos concederlos en los casos en que tenga sentido, sea una aplicación con cierta reputación y descargada de una fuente fiable.

Es posible acceder en cualquier momento al listado de aplicaciones con permiso de acceso a las notificaciones desde las Ajustes → Pantalla bloqueo y Seguridad → Notificaciones

6. Actualizaciones del sistema operativo y de las aplicaciones

Igual que sucede en los ordenadores, cada día se descubren vulnerabilidades y agujeros de seguridad que afectan igualmente a aplicaciones móviles como al propio sistema operativo del dispositivo.

Es por ello que igual que hacemos con nuestro ordenador y sus aplicaciones, **debemos de tener el dispositivo móvil y sus aplicaciones correctamente actualizadas**.

Ya que no resulta cómodo actualizar las aplicaciones "a mano" cada vez que surge una actualización nueva (pueden surgir varias a la semana dependiendo del número de aplicaciones que tengamos instaladas), lo más recomendable es activar las actualizaciones automáticas de las aplicaciones.

Esto se activa desde la aplicación
Google Play > Ajustes > Actualizar automáticamente > Actualizar las aplicaciones automáticamente solo a través de Wi-Fi.
Dado que la mayoría de usuarios disponen de una cantidad limitada de tráfico de

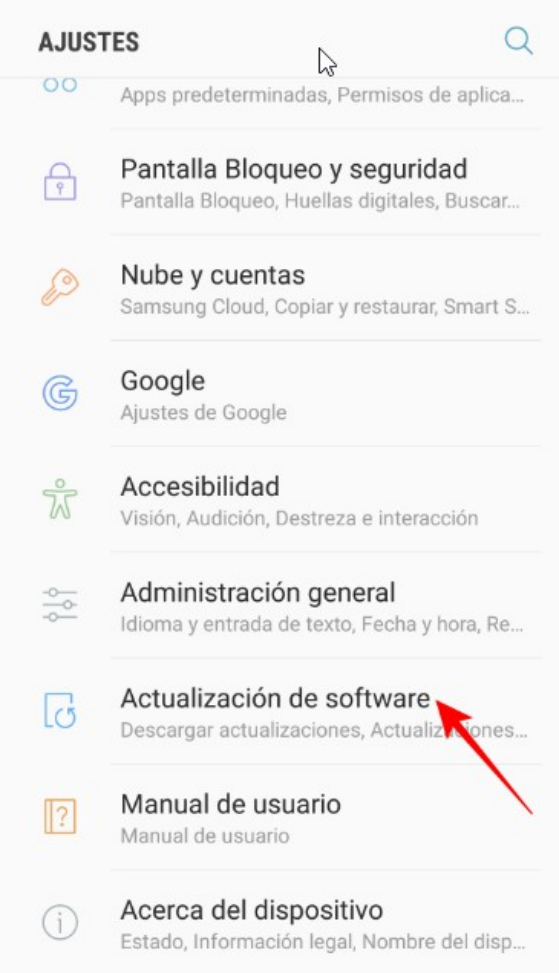
datos (conocidos coloquialmente como "megas") al mes, es recomendable activar la opción de que esta actualización se haga únicamente desde redes Wifi.

Todo esto afecta únicamente a las aplicaciones instaladas directamente desde Google Play, aunque el resto de tiendas de aplicaciones funcionan de forma similar, siendo posible que la propia aplicación sea quien nos avise.

En lo referente a las actualizaciones del sistema operativo, por desgracia no son tan sencillas de hacer: generalmente los fabricantes de los dispositivos móviles y las propias operadoras son reacios a actualizar los sistemas operativos a las últimas versiones para forzar al usuario a que cambie de terminal más a menudo.

Ante esta mala práctica, lo único que podemos hacer es informarnos de qué fabricantes o dispositivos móviles son más propensos a ser actualizados o comprar directamente los dispositivos "libres" que no vayan asociados a ningún operador, ya que estos acostumbran a ser más fácilmente actualizables.

Si se desea comprobar si tenemos la última versión que el fabricante u operadora han puesto a nuestra disposición, es posible comprobarlo desde Ajustes → Actualización de software.



En última instancia existe la opción de forzar la actualización reinstalando el sistema completamente, pero esto es una opción avanzada poco recomendable para la mayoría de usuarios.

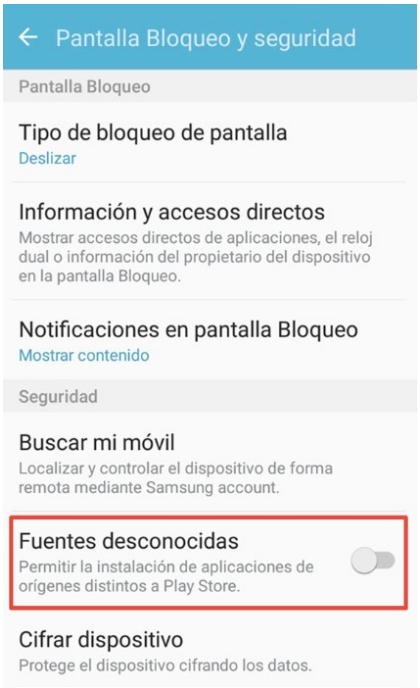
Debemos desinstalar todas aquellas aplicaciones que no estemos utilizando, ya que además de ganar espacio, evitamos sus actualizaciones y que tengan permisos de acceso a nuestro dispositivo.

7. Instalación desde fuera de Google Play

Aunque por norma general lo más común es instalar aplicaciones desde la aplicación Google Play, existe también la posibilidad de hacerlo desde aplicaciones externas como la tienda de Apps de Amazon, otras tiendas de dudosa reputación, o incluso descargando la aplicación directamente de Internet.

Si bien algunas de estas opciones son totalmente fiables (como la tienda de Apps de Amazon o las descargas de aplicaciones directamente desde las páginas de los desarrolladores), se debe ser extremadamente cauteloso con las aplicaciones descargadas de Internet, ya sea de páginas donde se comparten gratuitamente aplicaciones de pago o desarrolladores desconocidos que exponen sus aplicaciones.

Pese a que es poco recomendable descargar nada de fuentes no oficiales, si aun así decidimos hacerlo, debemos fijarnos muy bien en los permisos que pida la aplicación y descartar todas aquellas que necesiten más de lo estrictamente necesario: ubicación, leer contactos, leer y enviar SMS, hacer llamadas, activar la cámara, etc. También es muy recomendable analizar la aplicación con el antivirus, aunque hoy en día la mayoría de antivirus no detectan acciones peligrosas de aplicaciones móviles. Una buena opción es usar la web www.virustotal.com.



Para poder instalar aplicaciones desde fuentes no confiables deberemos activar la opción correspondiente desde Ajustes > Pantalla bloqueo y Seguridad > activar la opción de Fuentes desconocidas.

8. Evitar compras en aplicaciones

Por norma general al descargar aplicaciones desde Google Play es complicado hacer clic sin querer sobre una aplicación y comprarla por error, ya que se pide confirmación expresa antes de que la compra se realice, además de que siempre existe la posibilidad de devolver la aplicación en los minutos siguientes a la compra. No obstante, también es posible hacer compras directamente desde dentro de las aplicaciones, generalmente en juegos, donde a cambio de un pequeño micropago se consiguen monedas virtuales, vidas, cartones de bingo, armaduras, etc.

Este tipo de pagos son un gran peligro para nuestra cuenta corriente en caso de que dejemos un móvil o tablet a los más pequeños de la casa, ya que pueden no ser conscientes de estar haciendo compras con dinero real.

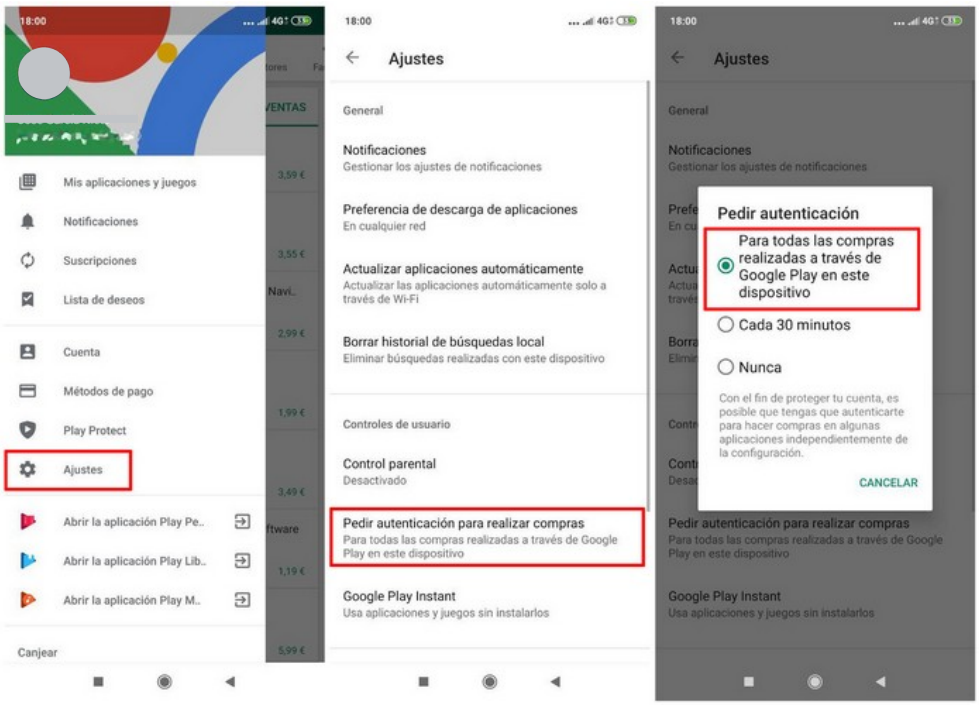
Para evitar esta situación u otros pagos involuntarios existe la posibilidad de obligar a introducir la contraseña de la cuenta de Google asociada al dispositivo para poder hacer cualquier tipo de pago, con lo cual nos evitaremos sustos en la factura.

Por defecto, es la opción que viene configurada, pero podemos comprobar que así lo tenemos, siguiendo los pasos que se indican a continuación:

1. Abre la aplicación Play Store.
2. En el menú, elige “Ajustes”.
3. “Pedir autenticación para realizar compras”.
4. Elegir “Para toda las compras realizadas a través de Google Play en este dispositivo”

Recuerda que para que sea efectivo y se eviten compras accidentales o automáticas, si alguna vez introduces la contraseña para comprar algo en la tienda de Google, nunca debes marcar la casilla “Recordar en este dispositivo”, ya que a partir de ese momento no te la volverá a solicitar y las compras podrán realizarse sin tu validación.

Debemos tener marcada esta opción en todos los dispositivos con Android en los que tengamos configurada nuestra cuenta de Google, tanto tablets como otros móviles.



9. Instalar teclados alternativos

Android permite utilizar infinidad de teclados además del que trae por defecto. Algunos de estos teclados nos permiten escribir más rápido, incluyen más caracteres, más emoticonos, o sencillamente se adecuan mejor a nuestro terminal o forma de escritura.

No obstante cualquier usuario que haya instalado un teclado diferente del original habrá visto un aviso que indica que se trata de una acción potencialmente peligrosa: esto es debido a que por la forma que tiene Android de utilizar teclados, si uno de ellos fuese malicioso podría capturar cualquier cosa que escribiéramos, incluyendo búsquedas, páginas web, o incluso contraseñas.

Es por ello que debemos, en la medida de lo posible, evitar utilizar teclados diferentes al original, o usar únicamente aquellos que tienen buena reputación y provienen de desarrolladores o empresas de renombre.

10. ¿Antivirus en el móvil?

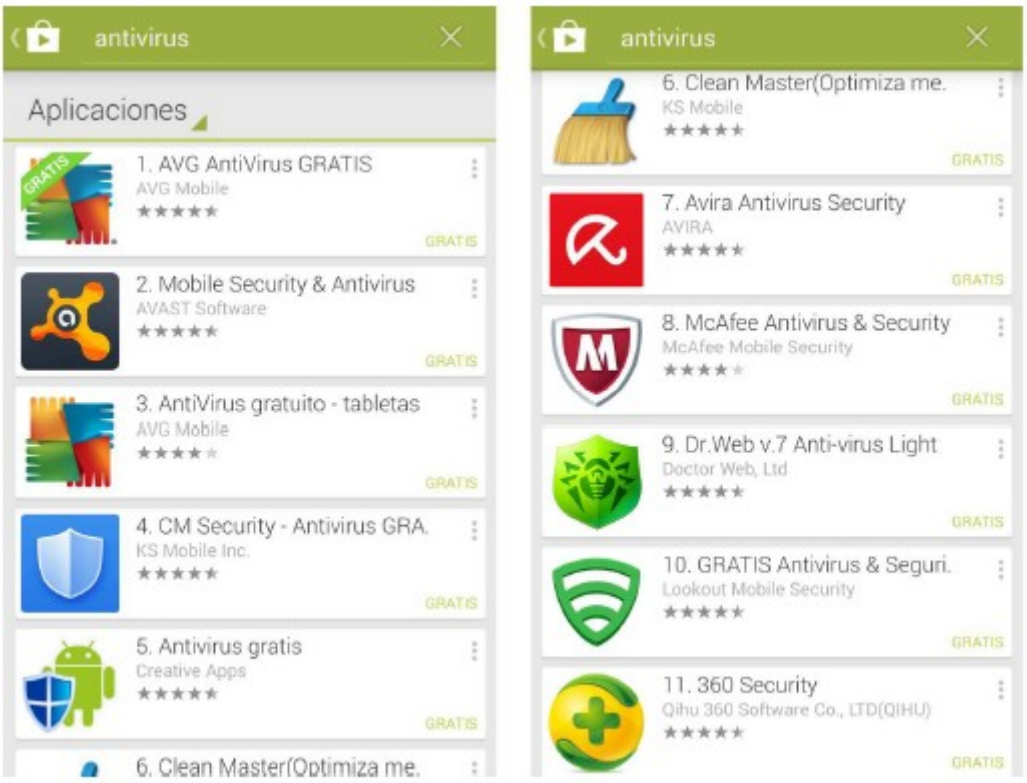
Dejamos para el final uno de los temas que más dudas causa entre los usuarios de dispositivos móviles: ¿hace falta instalar un antivirus?

De la misma forma que existen virus informáticos para ordenadores, existen virus informáticos para teléfonos inteligentes. Los creadores de virus cada día dedican más recursos a intentar infectar y comprometer los dispositivos móviles, ya sea para robar información, contraseñas, información personal, o sencillamente para controlarlos y

poder lanzar ataques desde estos, exactamente igual que con los ordenadores. El hecho de que casi todo el mundo tenga un teléfono propio el cual suele estar conectado a Internet todo el día, los convierte en un objetivo muy atractivo para este tipo de delincuentes.

Si bien es verdad que la forma de funcionar de los virus para móvil es muy similar a la de los ordenadores, en los móviles existen ciertas limitaciones en cuanto a la forma de propagación: la forma más común de infección es por descargar e instalar aplicaciones desde fuentes no fiables y en menor medida por abrir ficheros infectados.

Antivirus en Android:



Es cierto que los antivirus para móviles aún no son tan maduros como en los ordenadores convencionales, y que su utilización no garantiza que podamos instalar cualquier tipo de aplicación sin riesgo de infección, pero hoy por hoy, junto al sentido común, son el mejor arma que tenemos, así que la respuesta es SÍ, debemos instalar un antivirus en nuestro dispositivo móvil.

No obstante, recordemos que no por ello podemos bajar la guardia en el resto de buenas prácticas: no instalar aplicaciones de fuentes poco fiables (generalmente copias ilegales), no abrir ficheros sospechosos (correo, mensajería instantánea, Internet), y tener siempre tanto el sistema operativo como las aplicaciones lo más actualizadas posible.

11. 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:

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