¿Es tu móvil Android seguro? Revisa estos 10 consejos

La dependencia al 'smartphone' es tal que toda medida es poca si hablamos de ciberseguridad

ep / madrid 11.10.2017 | 18:39

La **dependencia del teléfono móvil** es tal que, prácticamente, podríamos considerarlo como una extremidad más de nuestro cuerpo. Y de exageración, nada, porque nos acompaña a todas horas -**se mete hasta en el baño y en la cama con nosotros**-. ¡Ay, si nuestro teléfono hablara! Y, ¡ay, si nuestro teléfono cae en otras manos! Toda medida es poca cuando hablamos tanto de ciberseguridad, especialmente en los **Android**.

Si eres de los asiduos al sistema operativo de Google, revisa este decálogo de recomendaciones descritas a continuación para comprobar si puedes mejorar la seguridad de la información almacenad en tu dispositivo.

Configura un PIN en la tarjeta SIM

Al igual que ocurre en los dispositivos iOS, el PIN impide el acceso no autorizado a los servicios de telefonía móvil asociados a la tarjeta SIM. Si se desconoce esta clave, solo es posible hacer llamadas de emergencias a números como el **112**.

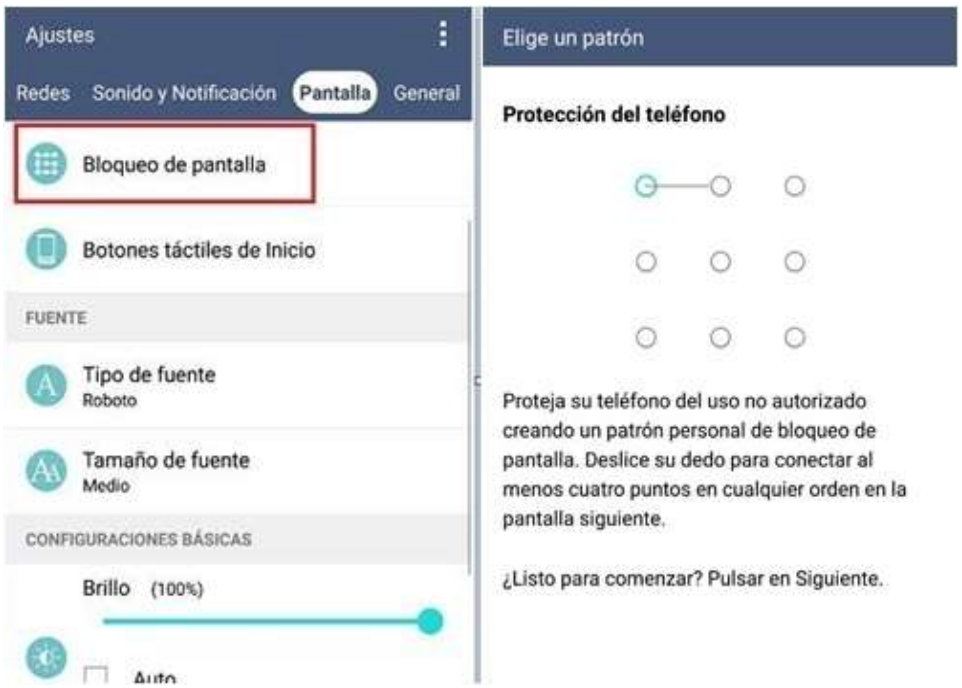
Android permite establecer un código PIN para la tarjeta SIM con un valor entre cuatro y ocho dígitos. Para modificar el PIN de nuestro dispositivo, es necesario acceder al menú **Ajustes > Seguridad > Bloqueo de tarjeta SIM > Cambiar PIN** de la tarjeta SIM, tal y como se muestran en las siguientes imágenes:

Se recomienda emplear una secuencia de números que no sea predecible, es decir, excluyendo valores como 0000, 1111 ó 1234, y emplear preferiblemente ocho dígitos.

Establece un código de acceso

Para evitar que nuestro dispositivo sea utilizado por una persona no autorizada, es recomendable configurar un código para bloquear el acceso no autorizado al terminal y, por tanto, también a sus comunicaciones, aplicaciones, datos... Dependiendo del modelo del dispositivo, se pueden establecer distintas vías de bloqueo, como son **patrones, códigos PIN, contraseñas** o detección biométrica de la huella dactilar.

A continuación, se muestra cómo bloquear el móvil estableciendo un patrón de desbloqueo. Esta opción está disponible desde **Ajustes > Seguridad > Bloqueo de pantalla:**



Configurar el bloqueo automático

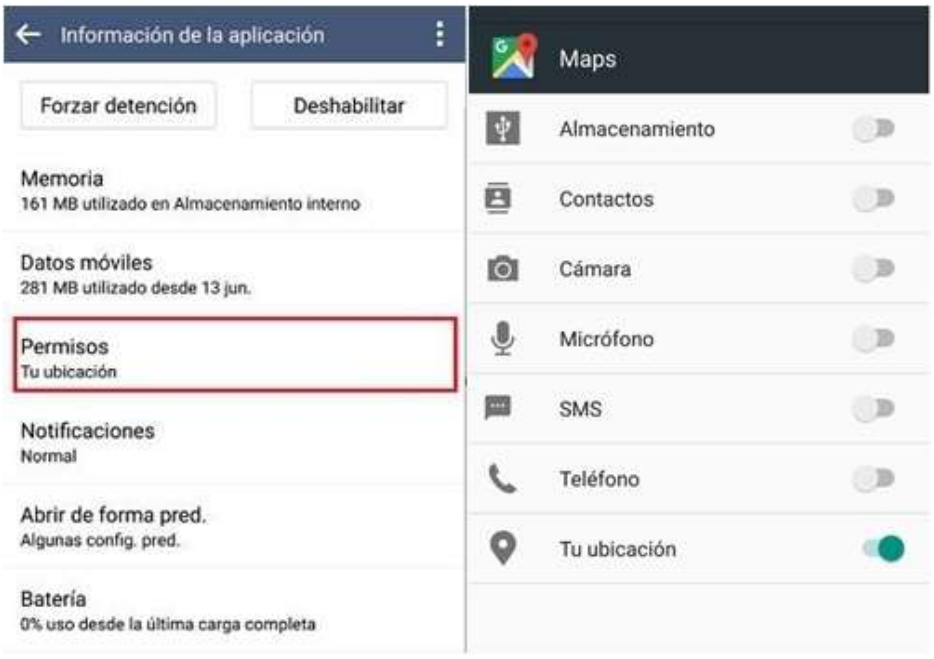
Es posible evitar que accedan a nuestro dispositivo sin autorización mediante el bloqueo automático del mismo transcurrido un tiempo predefinido por el usuario.

El tiempo de bloqueo de la pantalla del terminal se establece a través del menú **Ajustes > Seguridad > Bloqueo de pantalla > Temporizador de bloqueo**. Tal y como se puede ver en la imagen, es posible elegir entre distintos periodos de tiempo para bloquear automáticamente el dispositivo:

Permisos en aplicaciones

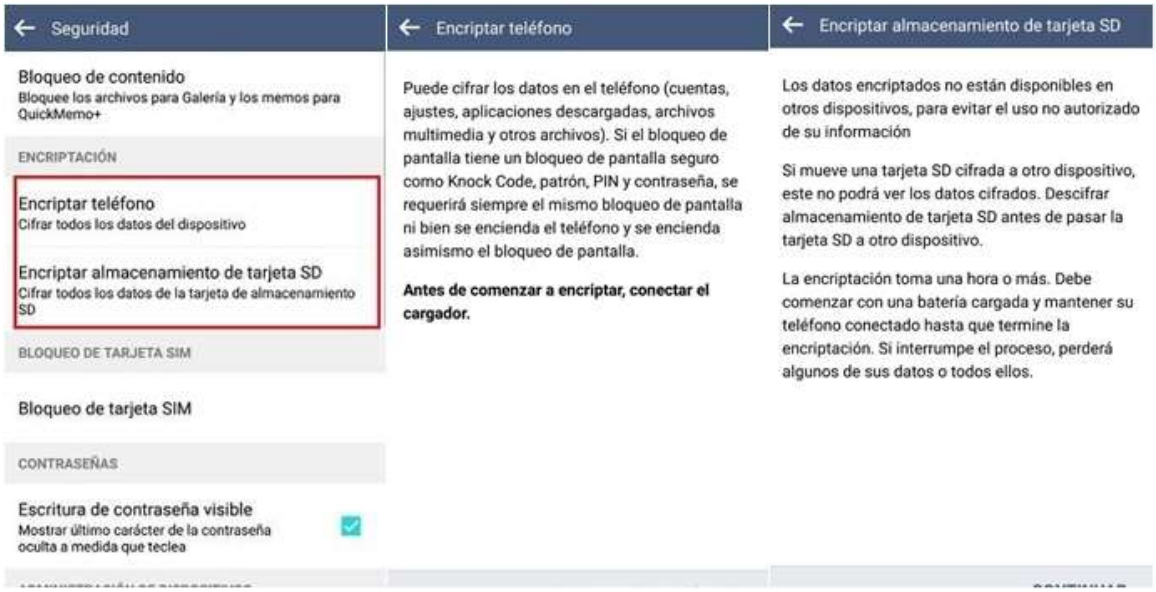
Al igual que ocurre en iOS, Android también permite deshabilitar los permisos de las aplicaciones instaladas en el dispositivo, puesto que en algunos casos estas solicitan más permisos de los necesarios para su correcto funcionamiento.

Android permite deshabilitar los permisos de las aplicaciones instaladas desde el menú Ajustes > Aplicaciones. Por ejemplo, en el caso de **Google Maps**, los permisos que se pueden habilitar o deshabilitar son los que se muestran a continuación:



Cifrado de datos

Nuestro dispositivo móvil contiene numerosa información importante, tanto a nivel personal como profesional, por lo que se recomienda que esta esté cifrada. Para cifrar el dispositivo es necesario acceder a la opción **Ajustes > Seguridad > Encriptar teléfono.** También se puede cifrar la tarjeta SD pulsando sobre Encriptar almacenamiento de tarjeta SD, disponible también desde la opción Seguridad.



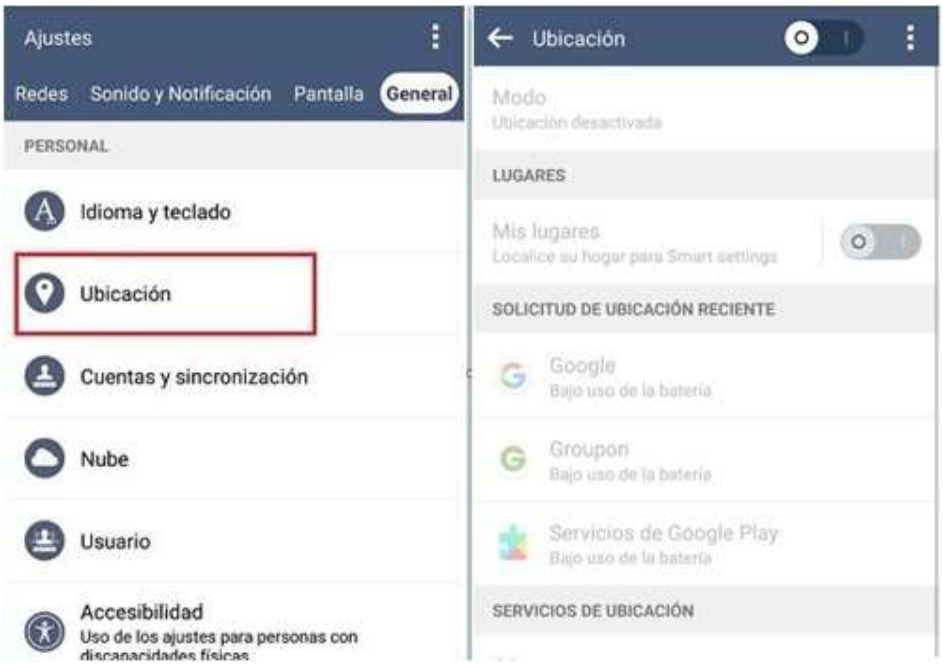
La codificación está basada en la fortaleza de la contraseña utilizada para cifrar los datos; es por ello que se aconseja utilizar una contraseña fuerte y que no sea predecible, como puede ser nuestro nombre o fecha de nacimiento.

Deshabilita conexiones cuando no las utilices

Existen numerosos ataques basados interceptar las comunicaciones, por lo que es recomendable habilitar las redes WiFi y Bluetooth solo cuando sea necesario. Para activar o desactivar la conexión WiFi, podemos acceder al menú **Ajustes > Redes,** tal y como se muestra en la siguiente imagen:

Si mantenemos la conexión WiFi habilitada permanentemente, es posible que nuestro dispositivo se conecte a redes inalámbricas no confiables. Además, se ha descubierto recientemente una vulnerabilidad denominada BlueBorne que afecta a millones de dispositivos y que puede provocar que un atacante infecte nuestro dispositivo con solo tener habilitada la conexión **Bluetooth**. Activa o desactiva tu conexión dependiendo de las necesidades que tengas desde **Ajustes > Redes.**

Es igualmente recomendable mantener deshabilitada la localización del dispositivo para evitar que las aplicaciones instaladas y distintos servicios web utilicen nuestra información geográfica sin nuestro consentimiento. Para activar o desactivar la localización, nos podemos dirigir al menú **Ajustes > General > Ubicación.**



Eliminación de datos del dispositivo móvil

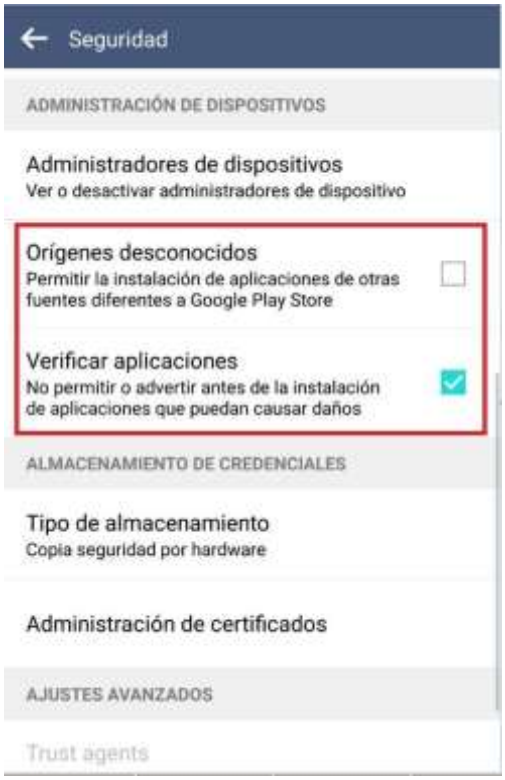
Android permite eliminar todos los datos del dispositivo desde **Ajustes > Copia de seguridad** y reinicio, ya que es importante eliminar toda la información del teléfono cuando lo cambiemos por otro o se lo demos a otra persona, puesto que nuestros dispositivos poseen numerosa información privada.

Además, es importante realizar una copia de seguridad de nuestros datos, para en el caso de pérdida o robo del terminal, dispongamos de los datos del teléfono. Para ello, es necesario acceder a la opción Copia de seguridad de datos desde el punto de menú mencionado anteriormente.

Descarga aplicaciones de Google Play Store

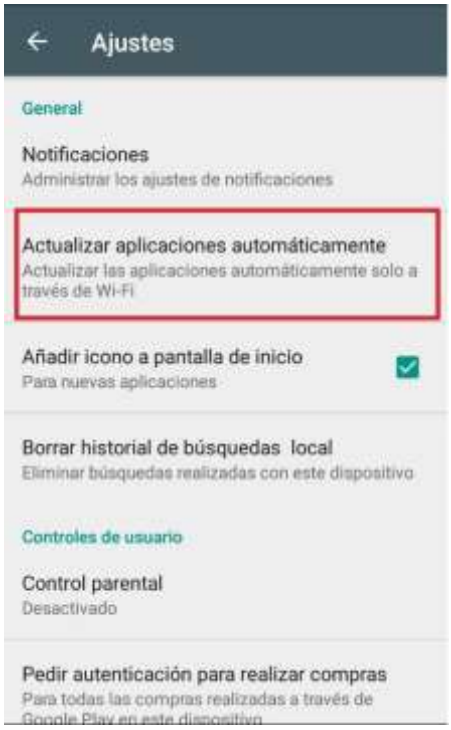
Los usuarios de Android pueden instalar aplicaciones desde plataformas o páginas web que podrían estar infectadas con 'malware', así que para disminuir las probabilidades de infección es recomendable no instalar 'apps' de fuentes desconocidas.

Para disminuir el riesgo de que nuestro dispositivo termine infectado, puedes desactivar la casilla Orígenes desconocidos y marcar Verificar aplicaciones. Ambas herramientas están disponibles desde el menú **Ajustes > Seguridad**, tal y como se muestra a continuación:



Mantén tu móvil actualizado

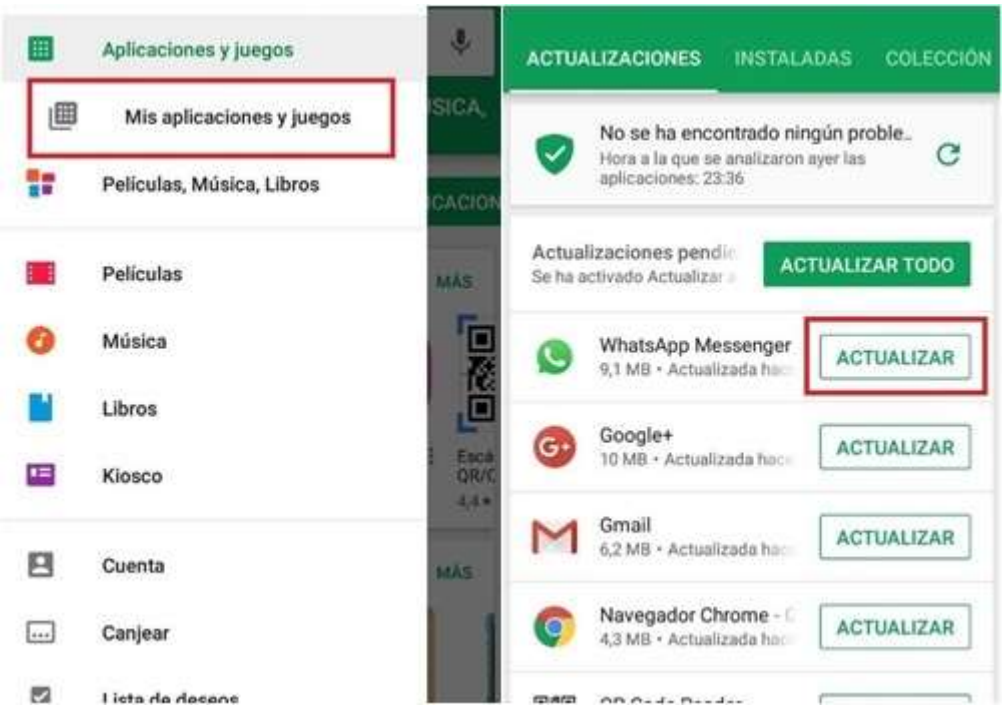
Para evitar que nuestro móvil posea vulnerabilidades conocidas que puedan ser utilizadas por los atacantes, es importante mantener las aplicaciones de nuestro dispositivo actualizadas a la última versión. Para ello, abre la aplicación Google Play Store, y a continuación pulsa en **Menú > Ajustes.**



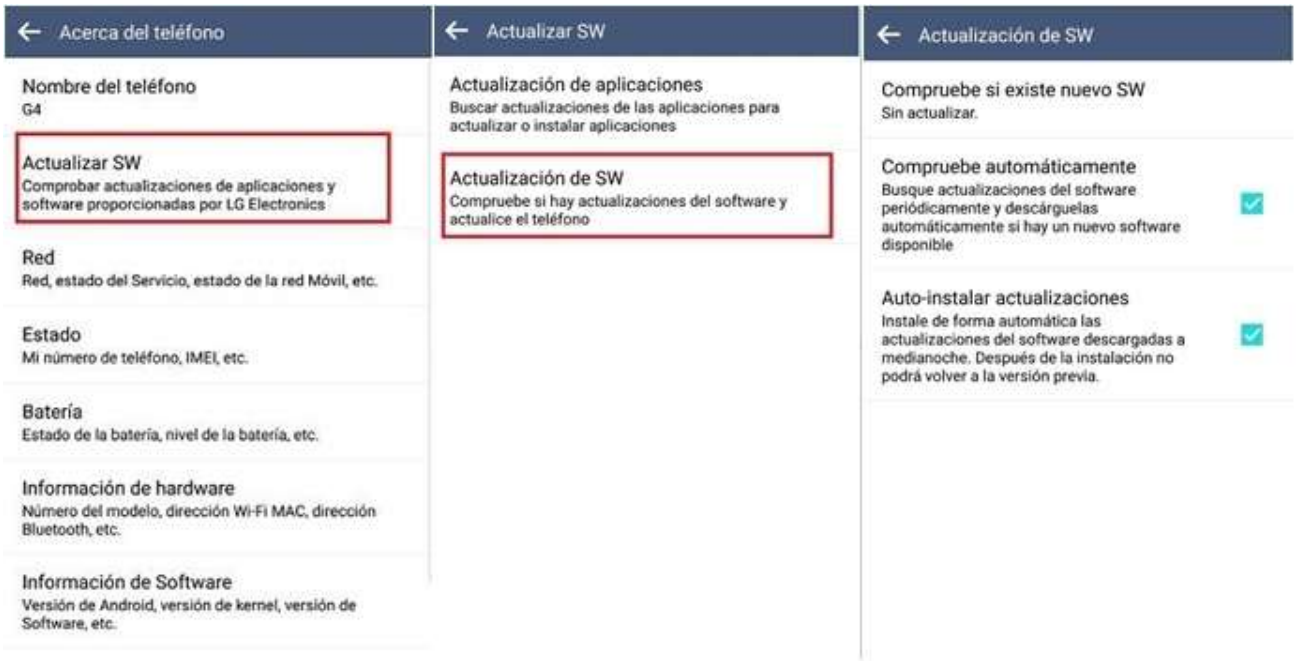
Las 'apps' pueden mantenerse actualizadas de forma automática en función de dos configuraciones disponibles: en cualquier momento, por lo que lo hará tanto si utilizas una conexión WiFi como datos móviles, o solo a través de WiFi, por lo que las aplicaciones se actualizarán **solo cuando el dispositivo está conectado a una red de este tipo.**

También se pueden actualizar las aplicaciones de forma individual desde el menú Mis aplicaciones y juegos, dentro de Google Play Store.

Aquellas aplicaciones que no estén actualizadas incluyen la opción Actualizar, tal y como se muestra:



Del mismo modo, es muy importante mantener actualizada la versión de Android a la última disponible para lograr un dispositivo más seguro, desde **Ajustes > Acerca del teléfono**.



No ´rootear´ el móvil

'Rootear' el 'smartphone' expone el móvil a las malas prácticas de terceros. Además, hay varios inconvenientes que son consecuencia de este proceso: elimina la garantía del fabricante, disminuye la seguridad de todos los datos almacenados o incluso **puede ocurrir que el teléfono se vuelva inestable** y hasta inservible si el proceso no es realizado de forma correcta.

Tomado de*:* www.europapress.es