ENJOY SAFER TECHNOLOGY™

Guía de seguridad para smartphones:

¿Cómo configurar tu Android de la forma más segura?

Índice

Introducción

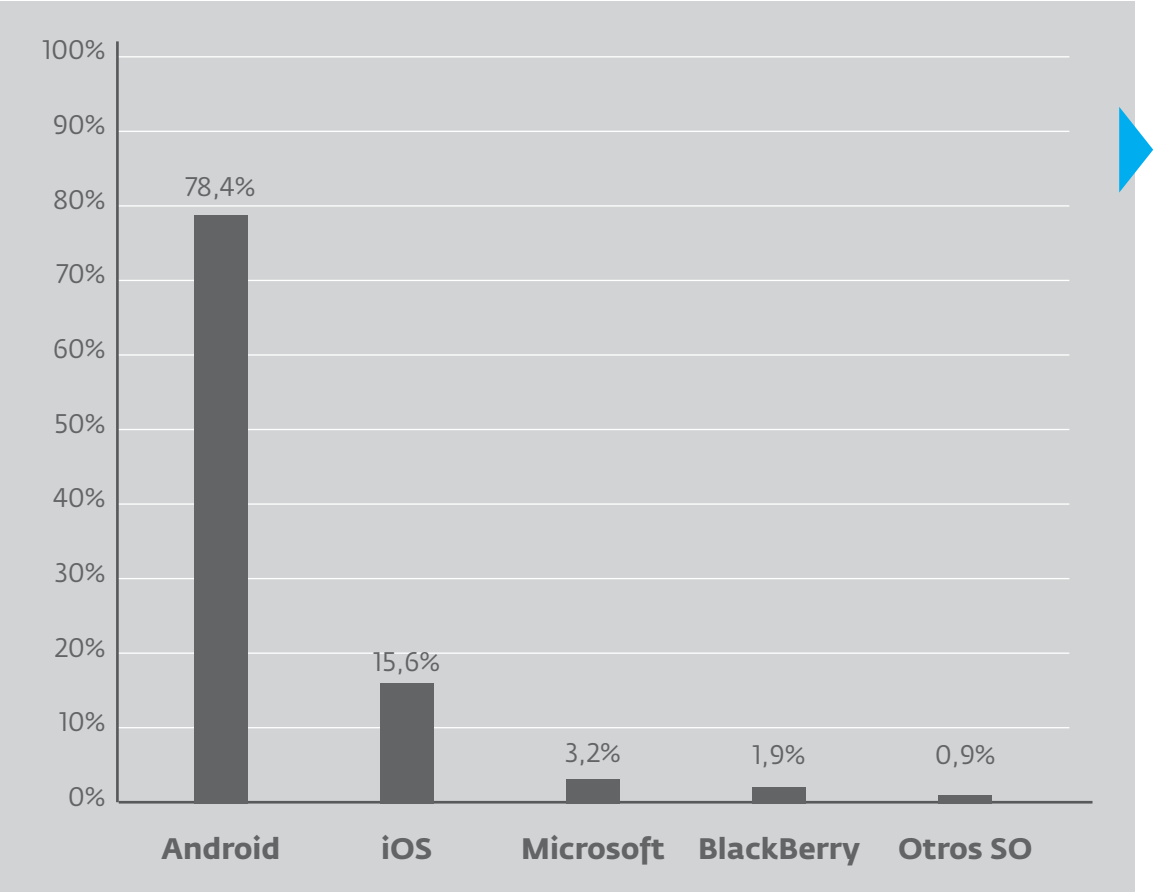
En los últimos años el mundo fue testigo de una evolución vertiginosa de la tecnología. Esto se nota, principalmente, en que la posibilidad de conectarse a Internet está literalmente al alcance del bolsillo, a través de dispositivos inteligentes lo suficientemente poderosos que hasta podrían superar a una computadora.

De esta manera, es posible manejar perfiles en las Redes Sociales, leer y responder *e-mails* y hasta realizar transacciones bancarias. No obstante, la masividad de estos equipos, y la gran cantidad de información relevante que manejan, hace que cada vez sean más tentadores para los ciberdelincuentes.

En este sentido, la concentración de tanta información sensible en un solo lugar, como puede ser un teléfono móvil, puede convertir a un usuario en una potencial victima si no se toman los recaudos necesarios.

Al observar las cifras del mercado de plataformas móviles, queda en evidencia que el sistema operativo Android es el más utilizado en todo el mundo, y es por esto que la presente guía apunta a explicar los aspectos más importantes a tener en cuenta a la hora de hacer las configuraciones de seguridad pertinentes en esta plataforma. De este modo, se podrán prevenir incidentes como ataques informáticos y robo de información.

Situación actual de Android en el mercado mundial



Según Gartner, una de las consultoras de TI más conocidas a nivel global, a fines de 2013 la población de plataformas móviles estaba compuesta por 78,4% de equipos con Android (758 millones de dispositivos), seguido por iOS con 15,6% (150 millones) y finalizando el podio está BlackBerry con 1,9% (18 millones).

Estos números demuestran la notable diferencia en la cuota de mercado, o *market share*, que posee Android frente a sus competidores. Debido a estos números resulta muy atractivo para los ciberdelincuentes atacar Android, ya que la cantidad de potenciales víctimas es muy amplia.

¿Qué tipo de amenazas pueden afectar a Android?

Como Android es la plataforma móvil más usada en todo el mundo, los ciberdelincuentes generan muchos códigos maliciosos para vulnerarla. Entre ellos, se pueden destacar casos de *malware* que suscriben al usuario a servicios de mensajería *premium*, además de que existen *botnets*, *adware* y troyanos, entre otras amenazas.

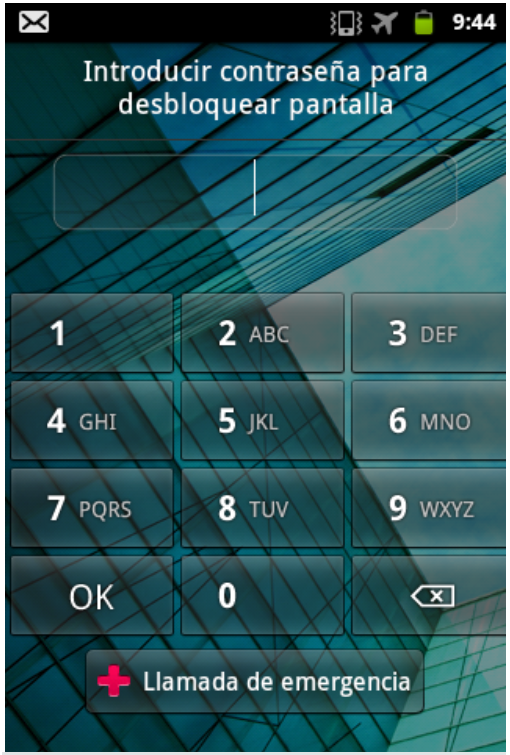
Algunos ejemplos concretos que se pueden destacar son troyanos como Geinimi, DroidDream y Raden que se ocultaban dentro de videojuegos. Raden, específicamente, es un troyano que se esconde en el popular "Buscaminas" y desde allí envía un mensaje de texto para suscribir al usuario a un servicio de mensajería *premium*. Luego, captura los mensajes de respuesta al usuario, de modo que nunca se entere de los gastos que le *está* ocasionando.

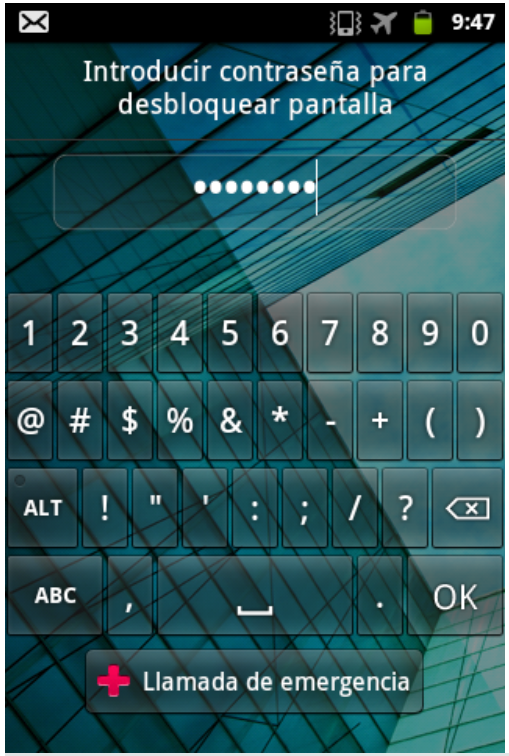
Además, se detectaron muchos casos de rogue, es decir, falsas soluciones de seguridad que prometen proteger el dispositivo cuando en realidad roban información o directamente no realizan ninguna acción preventiva.

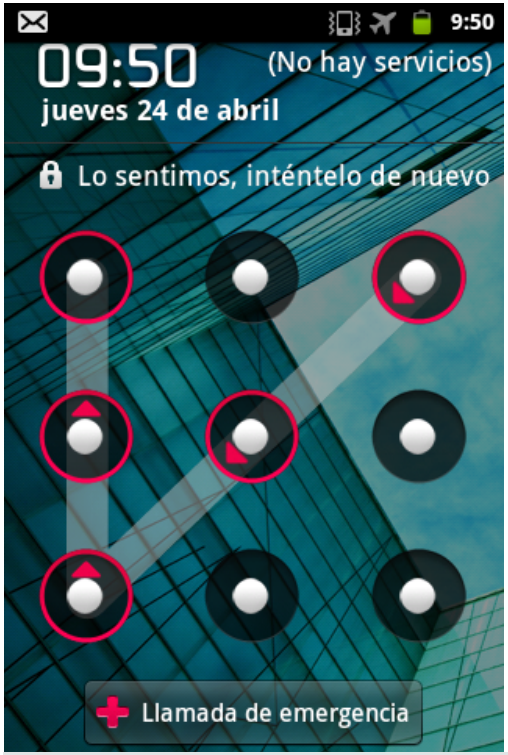
Configurando el acceso y bloqueo del dispositivo

A la hora de bloquear el dispositivo y, así, restringir el acceso a terceros no deseados, una de las mejores prácticas es utilizar una contraseña. Sin embargo, existen diferentes tipos de autenticación en Android.

Configurando el acceso y bloqueo del dispositivo







Clave numérica (PIN)

Permite configurar una contraseña numérica de cuatro dígitos.

Clave alfanumérica

Permite escribir frases con números, letras y caracteres especiales (también es requerida para cifrar el dispositivo).

Clave de patrón

Permite generar un patrón uniendo puntos.

Es recomendable configurarlo para que no se muestre el trazado, de esa forma nadie podrá ver exactamente la unión de puntos. Solo con deshabilitar la opción, el patrón dejará de ser visible.

La importancia de las actualizaciones

Las actualizaciones son fundamentales, ya que en algunas ocasiones van a definir si el equipo es vulnerable o no. A través de estas, los programadores corrigen errores, que podrían ser fallas de seguridad mediante las cuales un atacante podría ingresar al sistema, vulnerarlo y robar información.

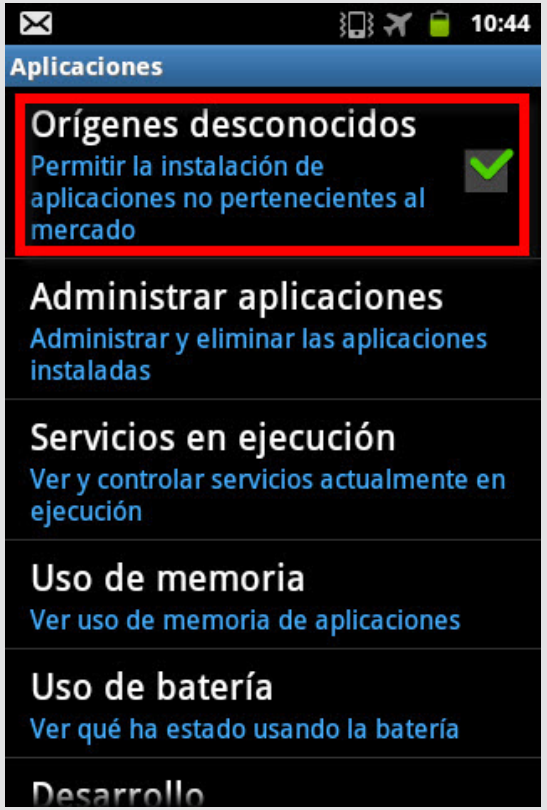
Para las actualizar de aplicaciones de terceros, se debe ingresar a Google Play, desde donde podrán descargarse las últimas versiones disponibles. Por otro lado, las actualizaciones oficiales de Android son administradas por cada compañía telefónica. Generalmente, cada vez que sale una actualización de sistema operativo, estas compañías envían un aviso a sus clientes, informando que se encuentra disponible una nueva actualización de modo que puedan descargarla.

Entonces, cada vez que una aplicación informa que una nueva actualización está disponible, es aconsejable leer primero qué problemas corrige y luego proceder a instalarla.

Las aplicaciones y sus permisos

A la hora de instalar aplicaciones en un dispositivo es necesario considerar dos puntos: su procedencia y los permisos que requieren. En primer lugar, siempre es recomendable utilizar repositorios oficiales y confiables para las descargas. A su vez, a la hora de instalar una aplicación desde Google Play, por ejemplo, inmediatamente se muestra una ventana con los permisos que solicita dicha aplicación. Es muy aconsejable leerlos y, de no estar seguro de lo que implican, evitar instalar la aplicación.

Cabe destacar que una aplicación podría estar infectada con *malware*, de modo que al instalarla seguramente exija la mayor cantidad de permisos posibles para operar libremente.



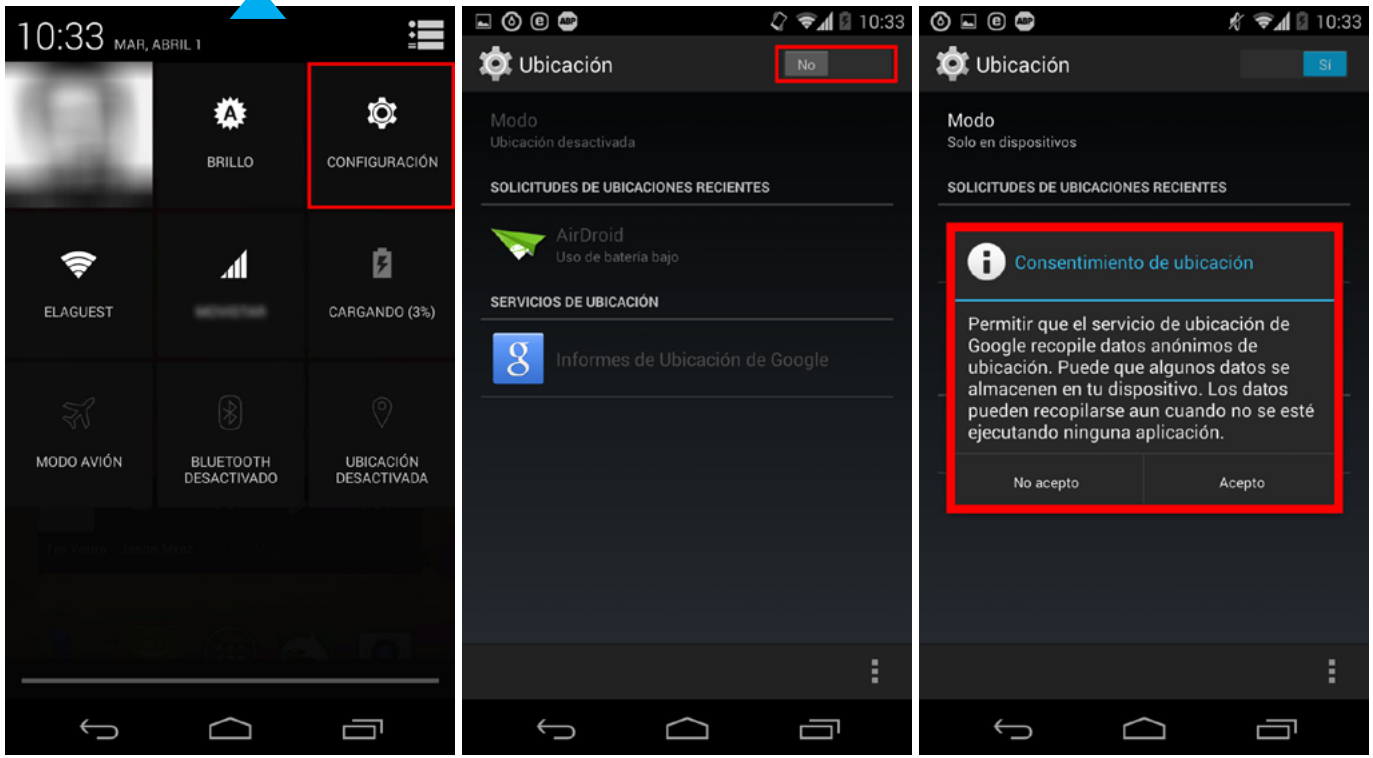
Tal como puede apreciarse en la imagen anterior, dentro del menú Configuración/ Aplicaciones se puede encontrar la opción para restringir aplicaciones desconocidas. Es recomendable desactivar esta opción, ya que limitará la instalación solo a aplicaciones de Google Play, reduciendo así el vector de ataque.

Evitando dejar la geolocalización al descubierto

Existen aplicaciones que solicitan activar la opción de geolocalización, es decir, un servicio que permite determinar la ubicación geográfica de un dispositivo mediante triangulación de coordenadas. Esta opción podría usarse, por ejemplo, para encontrar un dispositivo extraviado. No obstante, también puede ser aprovechado por ciberdelincuentes para conocer la ubicación de personas.

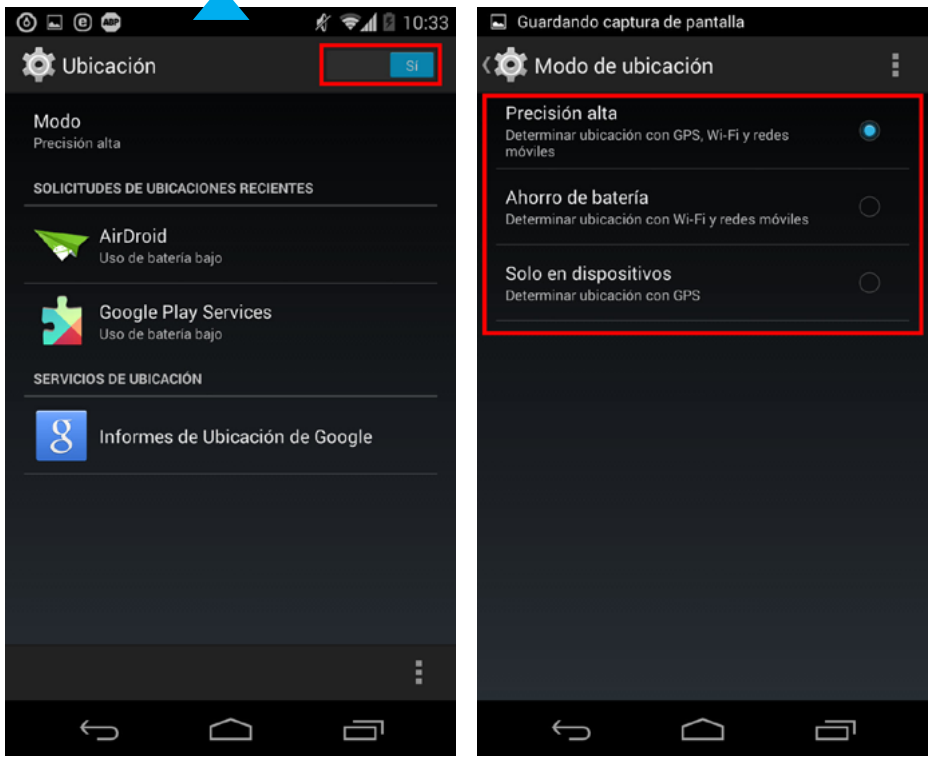
De modo que no es recomendable tener activada esta opción o, de hacerlo, verificar que los servicios que lo utilicen sean confiables y adecuados. Para configurar esta preferencia hay que ingresar al menú Ajustes/Ubicación y Seguridad/Mi ubicación, y desde allí es posible personalizar el posicionamiento mediante satélite GPS o Wi-Fi.

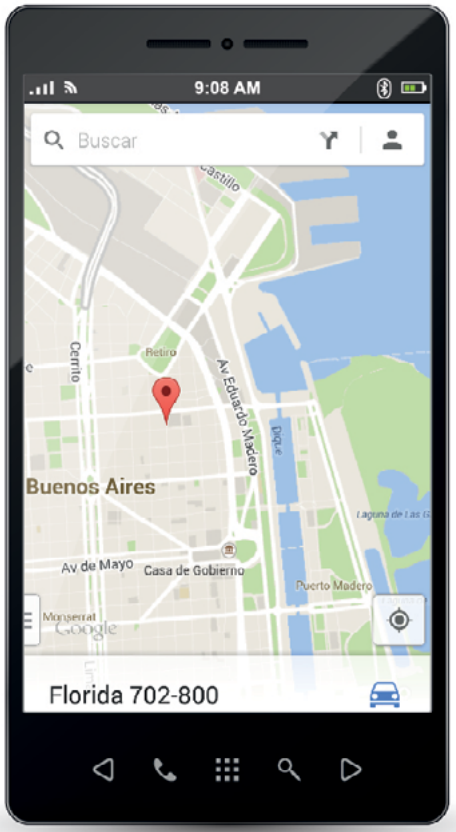
En la versión KitKat de Android se debe acceder a Configuración/Ubicación para habilitar, o no, el permiso de localización geográfica.



Evitando dejar la geolocalización al descubierto

Como puede apreciarse, una vez concedidos los permisos el equipo pedirá que se defina la exactitud de la ubicación.





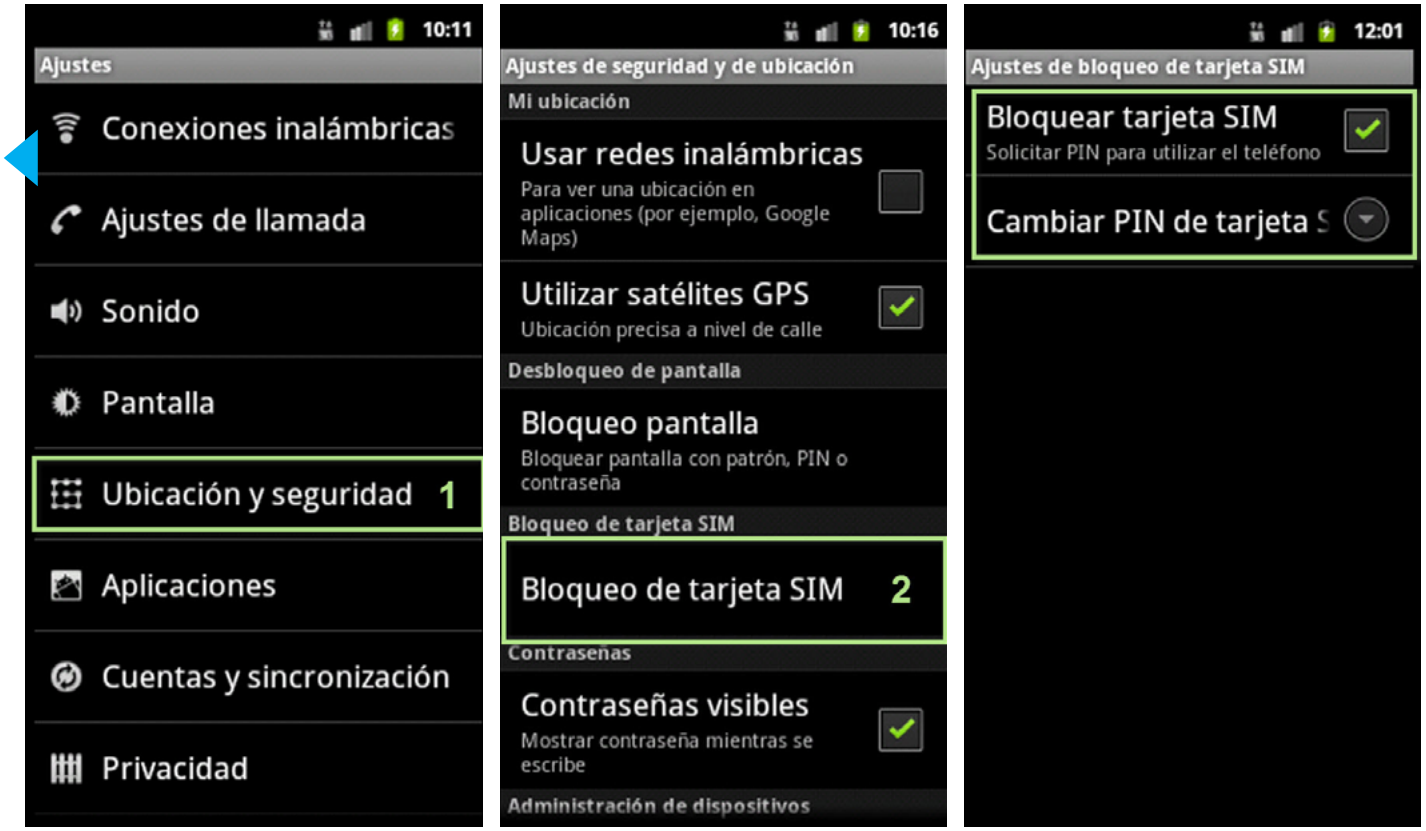
Protegiendo la Tarjeta SIM

No solo se debe bloquear el acceso al equipo, sino también a la tarjeta SIM, ya que puede prevenir la falsificación y robo de identidad. Es posible, entonces, utilizar una contraseña fuerte para que en el caso de perder el teléfono se puedan evitar casos como secuestros virtuales.

Vale destacar que el PIN en la tarjeta SIM no bloquea el acceso al teléfono, sino que lo hace con los servicios relacionados estrictamente al proveedor de la línea telefónica.

Otro punto no menor es que bloqueando la tarjeta SIM podemos prevenir números elevados en la facturación de la línea telefónica ya que si el equipo se pierde o fue robado y la tarjeta SIM no fue bloqueada previamente, el delincuente podría usar el servicio de telefonía indiscriminadamente, por ejemplo, haciendo llamadas de larga distancia o envíos sin control de mensajes de texto.

Configurar la tarjeta SIM para que solicite el PIN al usar el teléfono. Desde el mismo menú se puede cambiar el PIN de la SIM.



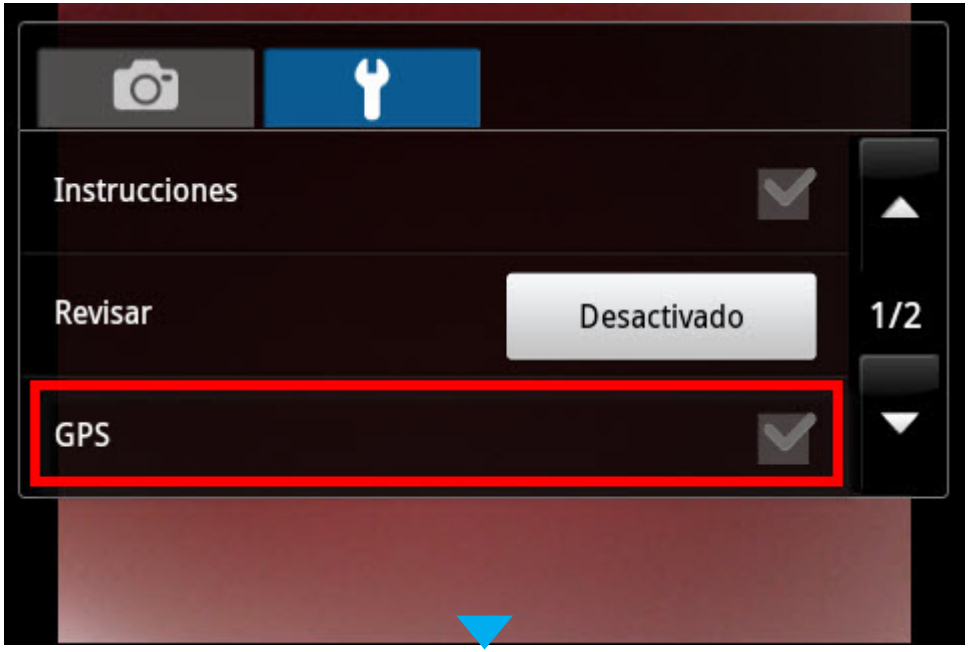
Las Redes Sociales como motor de Ingeniería Social

Los dispositivos móviles cuentan con conexión a Internet, por lo tanto deben tener las mismas consideraciones que se tienen para una computadora. Tal como sucede en una computadora, las Redes Sociales pueden ser grandes motores de Ingeniería Social para propagar códigos maliciosos. A la fecha se registran diferentes tipos de amenazas, como troyanos, *botnets* y *phishing*, que simulan ser aplicaciones o juegos para estas plataformas.

Es común que los atacantes usen Facebook y Twitter debido al alcance que tienen. A través de estas, suelen usar técnicas de Ingeniería Social para infectar con *malware* a sus víctimas o dirigirlos a sitios fraudulentos para robar información sensible, como credenciales e información bancaria.

Es por eso que es aconsejable no acceder a enlaces desconocidos, aunque sean compartidos por un contacto, ya que pueden haber sido productos de alguna aplicación maliciosa que infectó al contacto. En casos de tener duda si es real o no, es bueno preguntarle a la persona si lo que publicó es real o no, pero ante la duda siempre es aconsejable no ingresar.

Metadatos: las fotos dicen más que lo que muestran



Para modificar este servicio se debe acceder a la cámara del dispositivo y al botón de configuración; al acceder a este menú se debe desactivar la opción de GPS, tal como se ve a continuación.

A través de este proceso, las fotos no guardarán los metadatos de ubicación.

Los metadatos revelan información sobre datos; lisa y llanamente pueden indicar quién creó un archivo, la fecha y el modelo del equipo donde lo hizo, etc. Asimismo, pueden exponer las coordenadas geográficas donde fue tomada una fotografía, y en algunos casos hasta brindar el usuario y la contraseña de una sesión.

Este tipo de información resulta muy atractiva para los ciberdelincuentes con el objetivo de realizar ataques de Ingeniería Social dirigidos a una comunidad o grupo particular.

Es por esto que es recomendable desactivar la ubicación GPS para las fotografías, ya que en ocasiones, como durante vacaciones, se suelen compartir fotos directamente desde el dispositivo móvil y en ellas se podrían encontrar las coordenadas exactas de la foto. Esta información es muy valiosa para los cibercriminales, ya que les da la certeza de que el hogar de la víctima está vacío, por ejemplo.

Configurando la seguridad del navegador *web*

Algunas buenas prácticas para aplicar en el navegador *web* del dispositivo son:

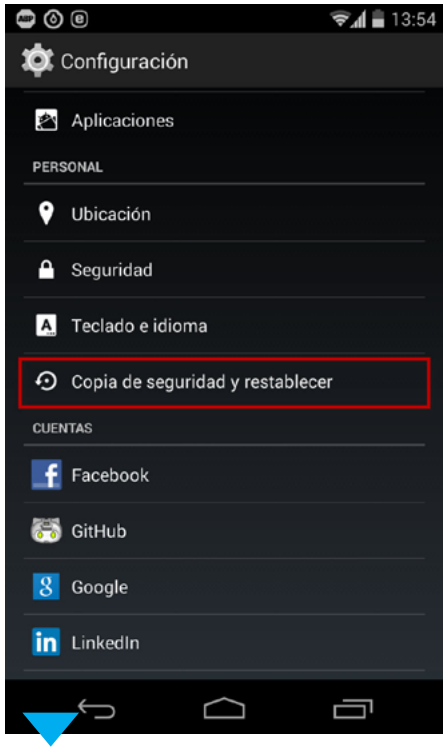
- **Contar con una solución antivirus capaz de analizar las conexiones y los archivos que se ejecutan.**
- **Deshabilitar ejecución de Java.**
- **Deshabilitar ejecución de Flash.**
- **Asegurarse de navegar siempre en sitios confiables con HTTPS.**
- **No visitar sitios desconocidos.**
- **Deshabilitar la opción Recordar contraseñas.**
- **Deshabilitar la opción Habilitar ubicación.**

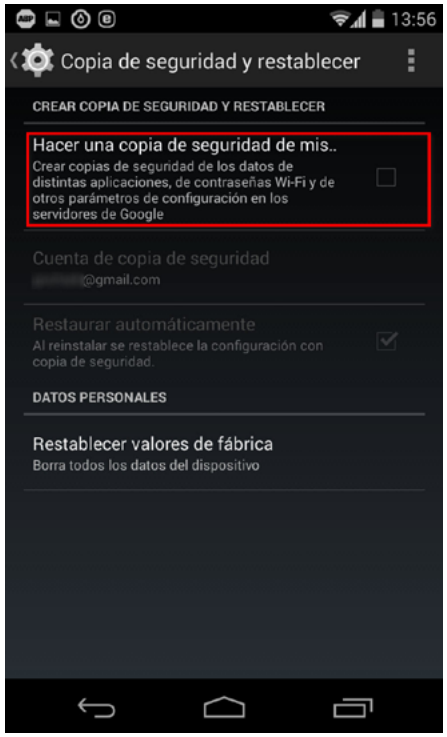
Estas recomendaciones ayudarán a prevenir ataques de *phishing* y *exploits* para los navegadores, y junto a una solución antivirus actualizada la información estará aún más segura.

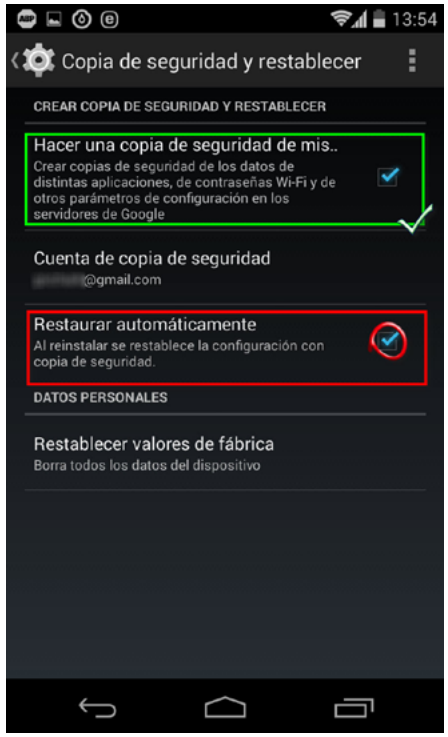
Creando copias de seguridad

Hacer copias de seguridad, o respaldos, de forma periódica es una muy buena práctica, ya que permitirán recuperar la información ante un incidente que la perjudique, borre o corrompa.

No hay una fórmula que indique qué archivos hay que incluir; cada usuario debe hacer una revisión de qué datos son más sensibles. Sin embargo, es interesante destacar el caso de, por ejemplo, los contactos, la agenda de correo, el calendario y los archivos personales como fotos y videos. Para hacerlo es necesario acceder al menú de configuración, una vez dentro, seleccionar la opción Copia de seguridad y restablecer.





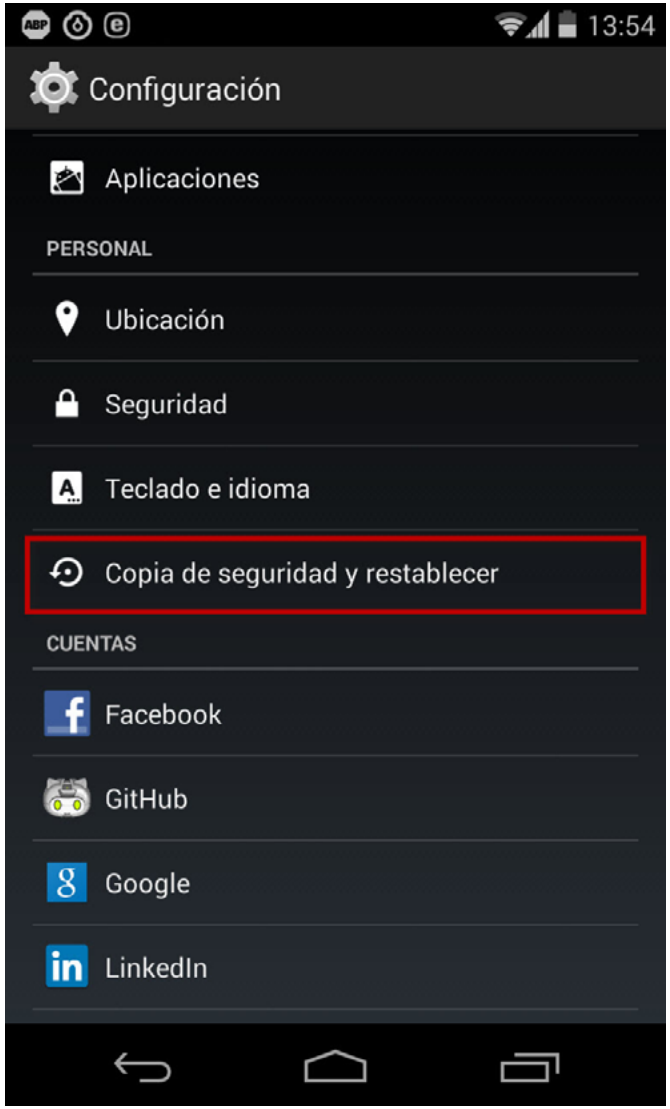


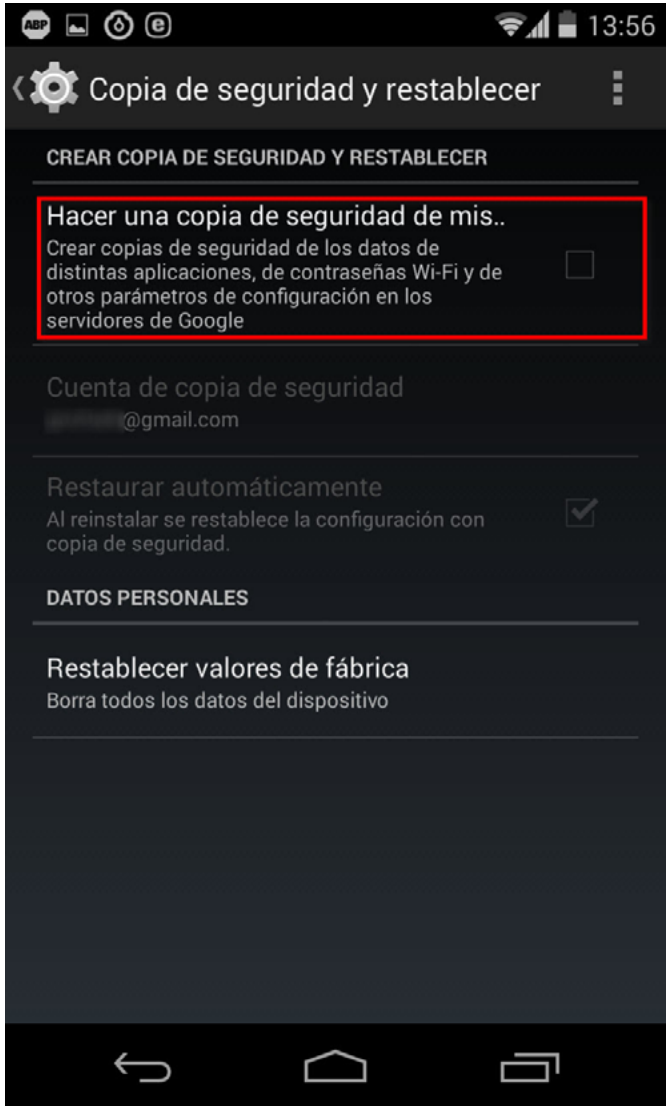
Como se aprecia en las capturas de pantalla, es recomendable marcar la opción Hacer una copia de seguridad de mis datos, para que los respaldos se ejecuten automáticamente. La opción de Restablecer automáticamente es opcional. Algo a tener en cuenta es las copias de seguridad realizadas son almacenadas en los servidores de Google, de modo que para realizar este procedimiento es necesario contar con una cuenta de Gmail sincronizada al equipo.

Cifrado de la información

La importancia de cifrar la información alojada en el dispositivo yace en que, al hacerlo, esta queda totalmente ilegible para cualquiera que no posea la clave para descifrarla, que es la misma que desbloquea el equipo.

Para este procedimiento debemos seguir los siguientes pasos:



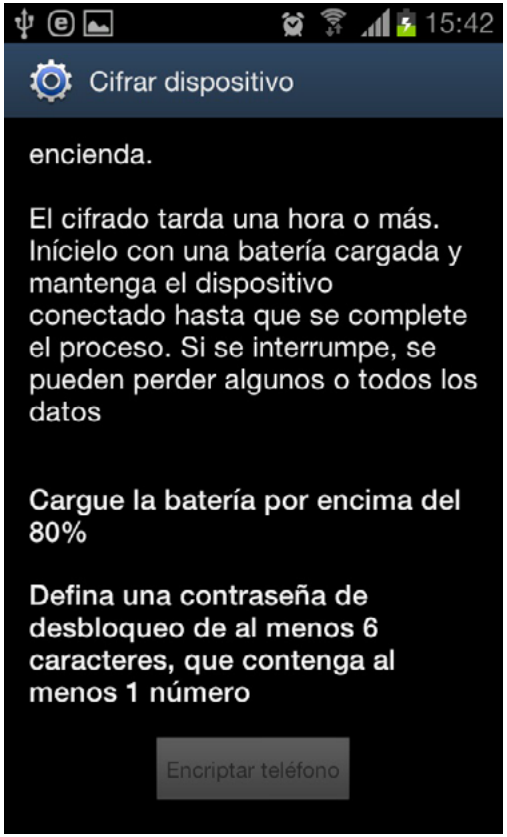


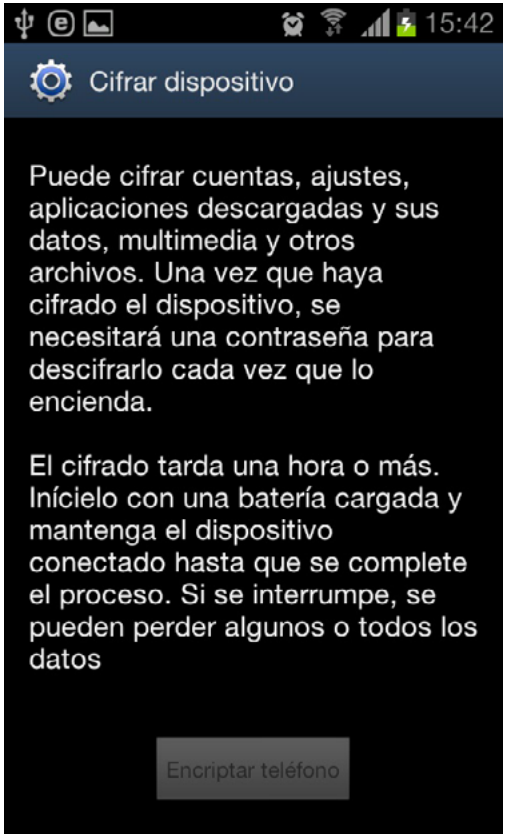
Cifrado de la información

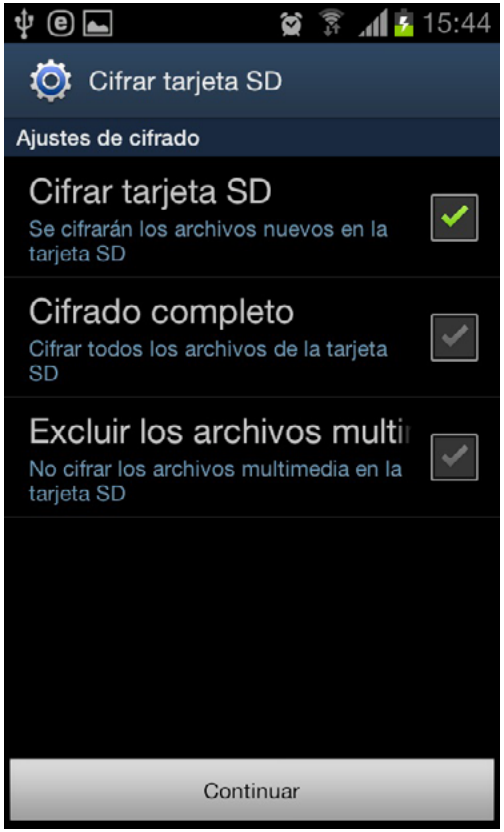
Como puede apreciarse, es posible cifrar la memoria SD y el dispositivo.

A* - Para cifrar el dispositivo es necesario contar con una clave alfanumérica. Además, el equipo solicitará tener la batería cargada al 80%; y este proceso puede durar más de una hora y no debe interrumpirse, o podría perderse alguno o todos los datos del dispositivo.

B* - La opcion para cifrar la tarjeta SD permite cifrarla por completo o solo algunos directorios, permitiendo cifrar tambien el contenido que se agrega posteriormente.







Administración remota

En algunos casos, es posible realizar ciertas acciones en el dispositivo remotamente, es decir, sin estar frente al equipo. La aplicación Android Device Manager de Google es un ejemplo de la utilidad de este servicio, especialmente en situaciones de robo y pérdida del equipo ya que, al tener conectividad Wi-Fi o 3g, este se conectará a la red y brindará su posición a través del GPS.

Otra de las grandes ventajas es el borrado de información remota, una opción que, generalmente a través de un portal *web*, permitirá acceder al dispositivo y borrar la información para que nadie pueda verla o robarla.

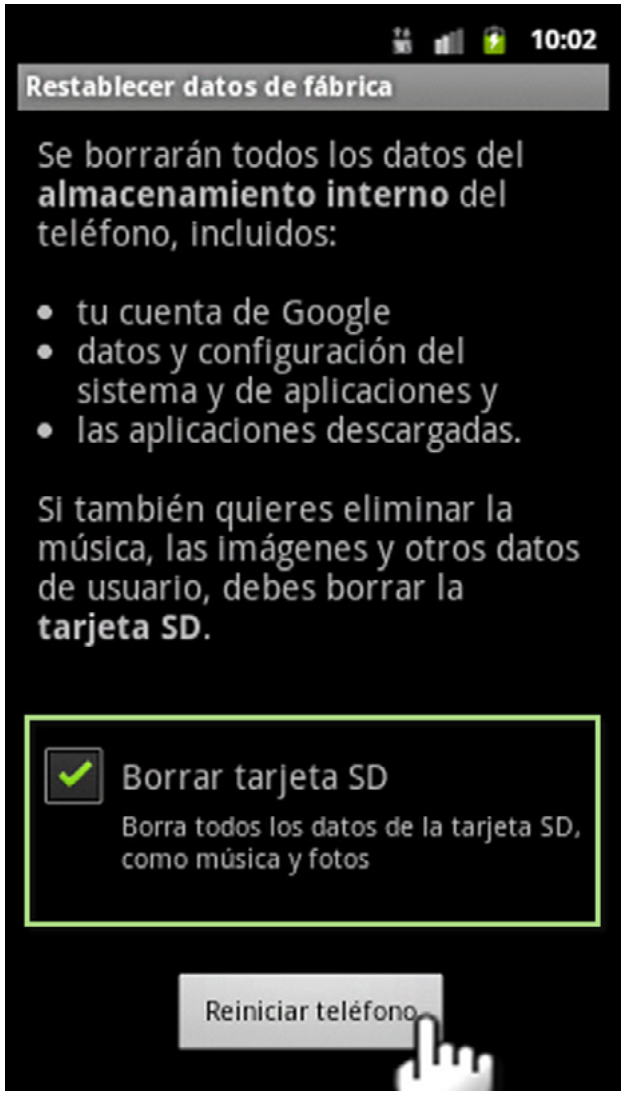
Asimismo, en caso de pérdida muchos equipos pueden emitir un sonido a modo de alarma para encontrarlo.

Borrado de datos a la hora de vender o regalar el dispositivo

Actualmente, la tecnología no solo es masiva, sino que evoluciona muy rápidamente. En este contexto, es muy común renovar los dispositivos en períodos cortos de tiempo y, en caso de que el viejo equipo sea vendido o regalado, es necesario tomar ciertas precauciones para evitar perder información en el proceso o que la misma sea accedida por personas que no deseamos que la tengan.

Principalmente, hay que borrar la información adecuadamente, pero no solo la que se encuentra en la memoria interna del equipo, sino también la que está alojada en la tarjeta SD, dado que por defecto es allí donde se guarda información personal como fotos y registros de conversaciones.

Para hacerlo es necesario ingresar en Ajustes/Privacidad y seleccionar Restablecer datos de fábrica. Al ejecutar la opción el equipo preguntará si se desea borrar la tarjeta de memoria, de modo que si la memoria también se entrega con el equipo es recomendable borrarla.



Conclusión

Como se expuso al comienzo de esta guía, la mayoría de la población posee equipos con Android que ya no se usan solo como teléfonos, sino que se han vuelto computadoras portátiles que caben en la palma de la mano y hasta ayudan a realizar las tareas cotidianas.

En este sentido, es aconsejable darle la importancia que se merece a la configuración de seguridad de un equipo, ya que al manejar tanta información sensible- como contraseñas, correos, datos bancarios e imágenes- en caso de robo o extravío se estaría perdiendo más que solo un aparato.

Además, si no se toman los recaudos necesarios en Internet, se podría perder el control del equipo en manos de riesgos virtuales que tienen poco, o nulo, interés en el *hardware*; solo buscan la información.

Al aplicar las buenas prácticas de esta guía la configuración de seguridad estará en un nivel muy alto, y si estas se complementan con una solución de seguridad se podrá lograr un estándar adecuado para el uso correcto del dispositivo con Android.

ENJOY SAFER TECHNOLOGY™

www.eset-la.com

/esetla

@esetla

/company/eset-latinoamerica