CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Buenas prácticas para el borrado seguro de dispositivos móviles

Documento Público

octubre 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. Introducción y objetivos

El presente breve documento pretende concienciar de la importancia de eliminar cualquier dato sensible de nuestros dispositivos móviles antes de desecharlos (regalar, vender, etc.), así como ofrecer recomendaciones para que cualquier usuario pueda eliminar los datos por sí mismo con garantías de seguridad suficientes.

2. Borra tus datos al cambiar de dispositivo

Por norma general los dispositivos móviles como tablets o teléfonos móviles, tienen un periodo de vida útil de entre 2 y 3 años el cual incluso se puede ver reducido por el avance de las tecnologías, averías, o directamente por el deseo de tener un nuevo terminal.

Un alto porcentaje de los dispositivos sustituidos van a parar a manos de amigos, familiares, otros usuarios corporativos, u organizaciones sin ánimo de lucro, por lo que debemos asegurarnos de eliminar toda información personal que no queramos que sea difundida:

- Fotografías y videos
- Agendas de contactos, calendarios y correos electrónicos
- Documentos descargados
- Aplicaciones con acceso a datos personales (redes sociales, almacenamiento en la nube, etc.)
- Contraseñas de acceso a sitios web y redes Wifi
- Historial de navegación y favoritos

Con el fin de evitar que olvidemos borrar alguno de estos datos, es recomendable que antes de dar, ceder, tirar o abandonar en un cajón nuestro terminal, nos aseguremos de hacer un borrado completo del mismo, de modo que además de no poder acceder a nuestros datos, el nuevo propietario encontrará el terminal como si viniese de fabrica y preparado para ser configurado a su gusto.

3. La necesidad de borrado seguro

Igual que sucede con discos duros o memorias USB, la información de los dispositivos móviles puede ser recuperada si no ha sido borrada de forma segura. Recuperar los datos borrados resulta tan sencillo que prácticamente equivale a no borrarlos, por lo que a continuación se incluyen los pasos a seguir para borrar los datos de forma segura en Android y iOS.

3.1 Borrado seguro en iOS

iOS incorpora una funcionalidad de borrado completo del dispositivo y restaurado a valores de fábrica, la cual hace que los datos no sean recuperables.

Los datos del dispositivo iOS son automáticamente cifrados y en el borrado, el dispositivo destruye la clave de cifrado, lo que hace imposible recuperar de cualquier

información del mismo.

Para hacer un borrado completo debemos acceder a ***Ajustes*** **>** ***General*** **> Restablecer > Borrar contenidos y ajustes**

Nótese que si el dispositivo dispone de código de bloqueo, éste será solicitado por lo que será necesario conocerlo.

Además la opción "Buscar mi iPhone" debe estar deshabilitada o se solicitará también el ID de Apple y la contraseña.

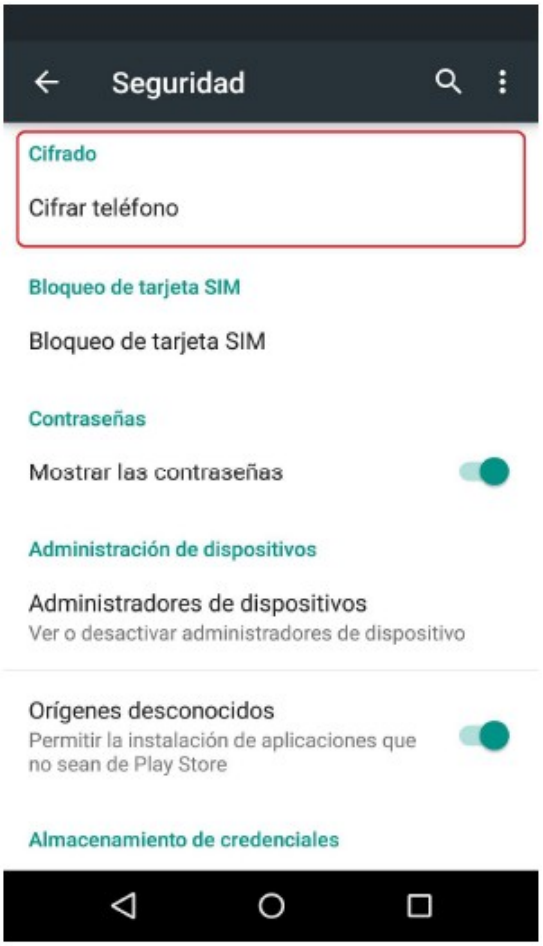
Esta opción se puede deshabilitar en ***Ajustes > iCloud > Buscar mi iPhone***.
Más información en la fuente oficial[1]

1 https://support.apple.com/es-es/HT201351

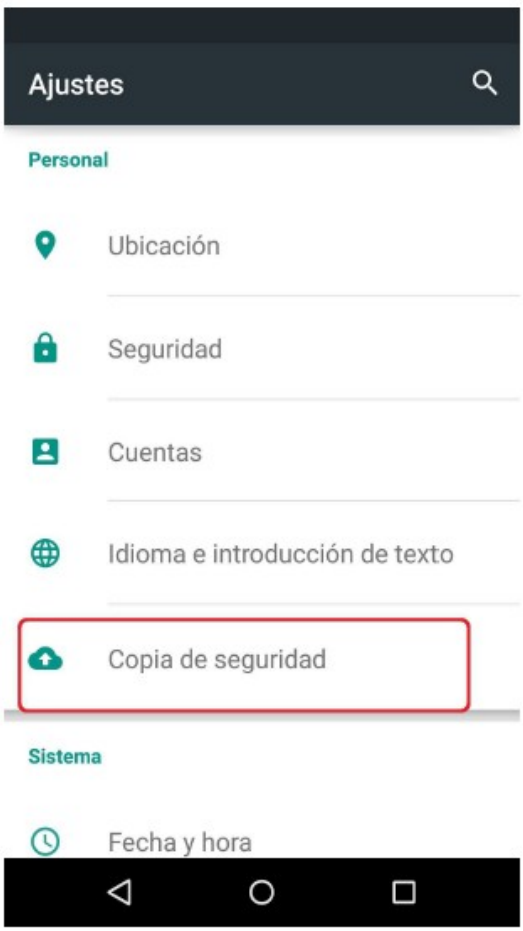
3.2 Borrado seguro en android

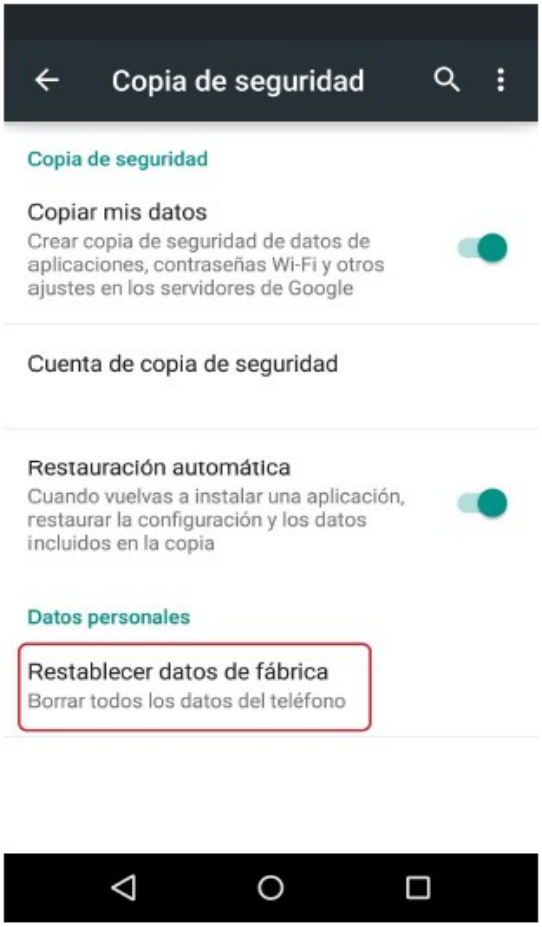
Para el borrado seguro de dispositivos Android utilizaremos también las propias herramientas que nos brinda el sistema operativo, aunque con ciertos matices ya que el restaurado de fábrica, por sí solo, no garantiza que los datos no vayan a poder ser recuperados:

Paso 1: acceder a ***Ajustes > Seguridad > Cifrar el teléfono.*** En versiones anteriores de Android aparece como *Encriptar teléfono*. Seguiremos los pasos indicados para cifrar el terminal.



Paso 2: acceder a ***Ajustes > Copias de seguridad > Restablecer los datos de fábrica > Restablecer teléfono***.





De esta forma habremos cifrado los datos (paso 1), destruido la clave de cifrado (paso 2).

4. Otras consideraciones

De igual forma que debemos eliminar la información del dispositivo, debemos tener especial precaución también con los datos almacenados en las tarjetas SIM (contactos y SMS), y en las tarjetas de memoria insertadas en los dispositivos, ya que es posible que olvidemos retirarlas antes de desechar el dispositivo.

5. 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:

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