

Buenas prácticas para el borrado seguro de dispositivos móviles

Documento Público



**GENERALITAT
VALENCIANA**



Unión Europea

Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Sobre CSIRT-cv

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.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

CSIRT-cv ha certificado su Sistema de Gestión de Seguridad de la Información con AENOR según la norma UNE-ISO/IEC 27001:2007 cuyo alcance son los sistemas de información que dan soporte a los servicios prestados a la Generalitat Valenciana para la prevención, detección y respuesta antes incidentes de seguridad en las TICs.



Datos de contacto

CSIRT-cv Centro de Seguridad TIC de la Comunitat Valenciana

<http://www.csirtcv.gva.es/>

<https://www.facebook.com/csirtcv>

<https://twitter.com/csirtcv>

Licencia de uso

Este documento es de dominio público bajo licencia Creative Commons Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.



Índice de contenido

1.	Justificaci3n	4
2.	Borra tus datos al cambiar de dispositivo.....	4
3.	La necesidad del borrado seguro	5
3.1.	Borrado seguro en Blackberry OS	5
3.2.	Borrado seguro en iOS	6
3.3.	Borrado seguro en Android.....	8
4.	Otras consideraciones a tener en cuenta	10
5.	Contacto y consultas.....	10

1. Justificación

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 del 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, iOS (Apple) y Blackberry OS.

3.1. Borrado seguro en Blackberry OS

Blackberry dispone de la posibilidad de borrar de forma segura el terminal sin necesidad de instalar aplicaciones de terceros.

Para ello bastará con encontrar en las opciones del terminal la opción *Borrado de seguridad*.

Dependiendo de la versión del dispositivo, esta opción estará en *Configuración > Seguridad y privacidad*, o en *Configuración > Seguridad > Borrado de seguridad*.

Es posible que tras pulsar sobre *Borrado de seguridad* se nos pida que introduzcamos un texto como confirmación de que estamos de acuerdo, así como que marquemos si deseamos borrar todos los datos y aplicaciones o solo parte.

Se dispone de más información en la fuente oficial:

<http://btsc.webapps.blackberry.com/btsc/viewdocument.do?noCount=true&externalId=KB14058>

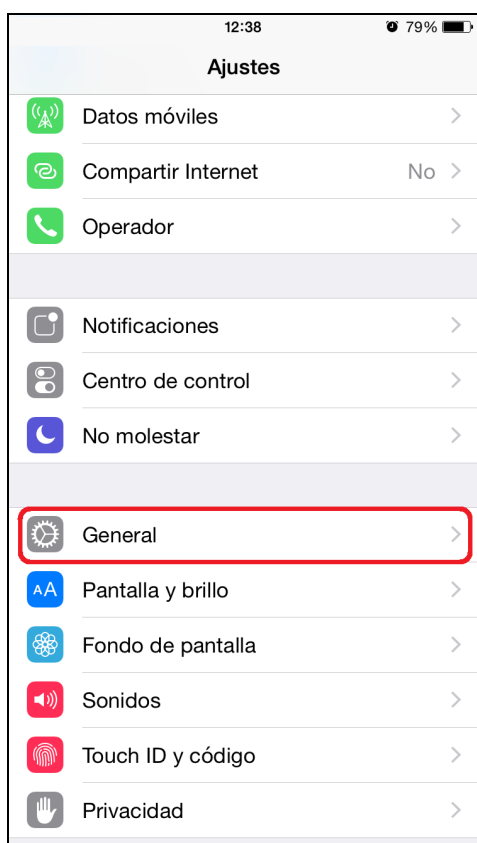
<http://btsc.webapps.blackberry.com/btsc/viewdocument.do?noCount=true&externalId=KB33591>

3.2. 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*.

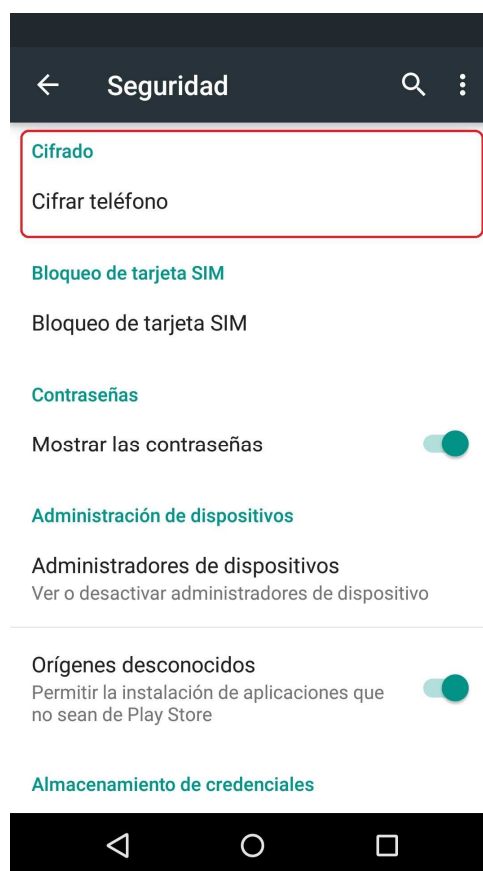
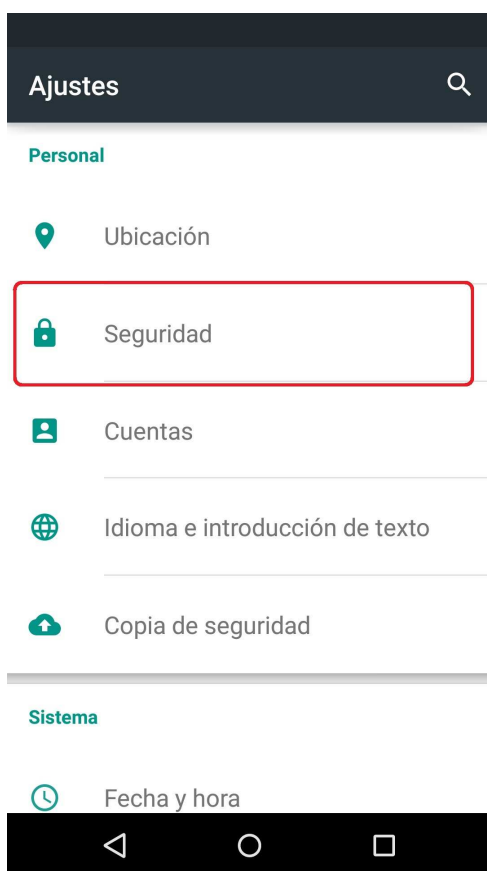
Más información en la fuente oficial:

<http://support.apple.com/es-es/HT5661>

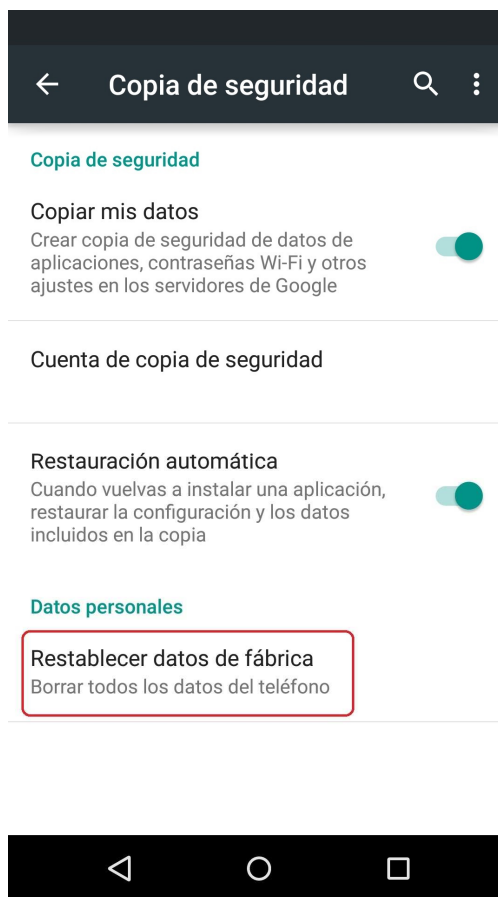
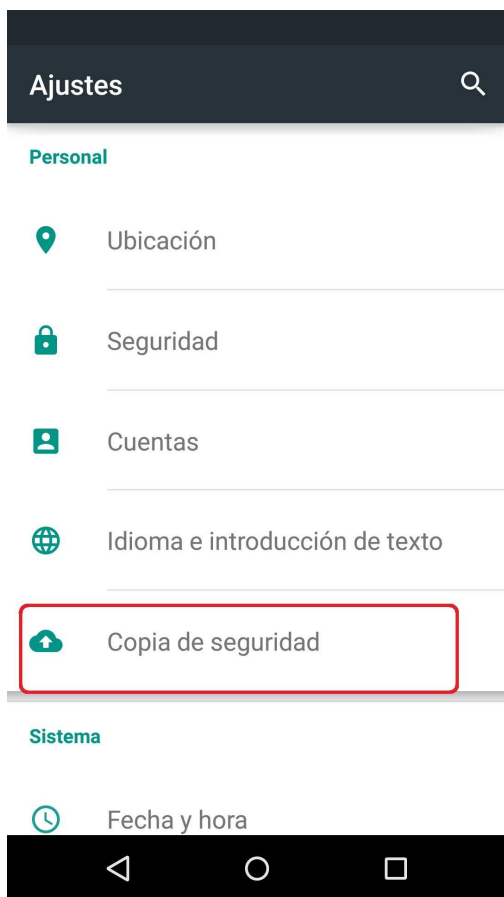
3.3. Borrado seguro en Android

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 a tener en cuenta

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:

<http://www.csirtcv.gva.es/>

<https://www.facebook.com/csirtcv>

<https://twitter.com/csirtcv>