USO SEGURO Dispositivos móviles y MEDIDAS DE PRECAUCIÓN

SEMINARIO ONLINE 1

ÍNDICE

INTRODUCCIÓN

El fenómeno del uso de los teléfonos inteligentes y tabletas, está teniendo como protagonistas a los niños y adolescentes.

Son muchos los menores que acceden desde los dispositivos de sus padres o tutores. Utilizando así aplicaciones de juegos, dibujos, fotografías, etc.

Y los adolescentes que poseen estos dispositivos, los utilizan a diario para estar en conexión permanente a Internet, mensajería instantánea y redes sociales.

Por ello, es necesario fomentar la concienciación para un uso seguro y responsable de estos aparatos.

Y la educación sobre un uso inteligente de estos dispositivos, comienza desde la propia familia. Cuya responsabilidad es educar sobre su uso responsable mediante unas normas de uso y la supervisión correspondiente de la utilización que hacen de ellos los menores.

CyL digital

Junta de Castilla y León

MÓDULO 1

CONSEJOS PARA PADRES Y TUTORES SOBRE EL USO DE DISPOSITIVOS MÓVILES

CONSEJOS DE USO DE DISPOSITIVOS MÓVILES

Los menores tienen una gran facilidad para aprender y manejar los dispositivos móviles (smartphones y tablets). Y a esto se suma el gran atractivo que suponen por su infinidad de utilidades.

Por ello, la orientación, apoyo y supervisión de la familia para que se mejore el uso de estos aparatos es uno de los objetivos a conseguir.

Los especialistas de la Brigada de Investigación Tecnológica (BIT), hacen una serie de recomendaciones para los padres y tutores sobre su uso.

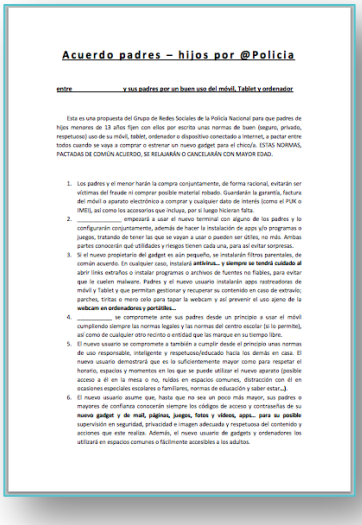
- Llegar a un acuerdo común sobre las normas de utilización de estos aparatos por parte de los menores.

- Supervisar lo que hacen con el móvil, cómo y con quién así como participar en la elección del terminal que realmente necesitan.

- Explicar las medidas de seguridad y prevención generales para evitar problemas como el Ciberbullying o el Grooming.

- Formar y concienciar a los menores de la importancia de la privacidad y los riesgos de seguridad con la premisa fundamental de su uso con responsabilidad.

- Recordar y hacer hincapié a los menores y adolescentes que sean especialmente cuidadosos con fotos, vídeos y contenidos que comparten.



Acuerdo padres – hijos por @Policia

entre _____ y sus padres por un buen uso del móvil, Tablet y ordenador

Esta es una propuesta del Grupo de Redes Sociales de la Policía Nacional para que padres de hijos menores de 13 años fijen con ellos por escrito unas normas de buen (seguro, privado, respetuoso) uso de su móvil, tablet, ordenador o dispositivo conectado a internet, a pactar entre todos cuando se vaya a comprar o estrenar un nuevo gadget para el chico/a. ESTAS NORMAS, PACTADAS DE COMÚN ACUERDO, SE REAJUSTARÁN O CANCELARÁN CON MAYOR EDAD.

1. Los padres y el menor harán la compra conjuntamente, de forma racional, evitarán ser víctimas del fraude ni comprar posible material robado. Guardarán la garantía, factura del móvil o aparato electrónico a comprar y cualquier dato de interés (como el PUK o IMEI, así como los accesorios que incluya, por si luego hiciesen falta.
2. _____ empezará a usar el nuevo terminal con alguno de los padres y lo configurarán conjuntamente, además de hacer la instalación de apps y/o programas o juegos, tratando de tener las que se vayan a usar o pueden ser útiles, no más. Ambas partes conocerán qué utilidades y riesgos tienen cada una, para así evitar sorpresas.
3. Si el nuevo propietario del gadget es aún pequeño, se instalarán filtros parentales, de común acuerdo. En cualquier caso, instalará **antivirus... y siempre se tendrá cuidado al** abrir links extraños o instalar programas o archivos de fuentes no fiables, para evitar que le caelen malware. Padres y el nuevo usuario instalarán apps rastreadoras de móvil y Tablet y que permitan gestionar y recuperar su contenido en caso de extravío; parches, tiritas o mero celo para tapar la webcam y así prevenir el uso ajeno de la **webcam en ordenadores y portátiles...**
4. _____ se compromete ante sus padres desde un principio a usar el móvil cumpliendo siempre las normas legales y las normas del centro escolar (si lo permite), así como de cualquier otro recinto o entidad que las marque en su tiempo libre.
5. El nuevo usuario se compromete a también a cumplir desde el principio unas normas de uso responsable, inteligente y respetuoso/educado hacia los demás en casa. El nuevo usuario demostrará que es lo suficientemente mayor como para respetar el horario, espacios y momentos en los que se puede utilizar el nuevo aparato (posible acceso a él en la mesa o no, ruidos en espacios comunes, distracción con él en ocasiones especiales escolares o familiares, normas de educación y saber estar...).
6. El nuevo usuario asume que, hasta que no sea un poco más mayor, sus padres o mayores de confianza conocerán siempre los códigos de acceso y contraseñas de su **nuevo gadget y de mail, páginas, juegos, fotos y vídeos, apps... para su posible** supervisión en seguridad, privacidad e imagen adecuada y respetuosa del contenido y acciones que este realice. Además, el nuevo usuario de gadgets y ordenadores los utilizará en espacios comunes o fácilmente accesibles a los adultos.

Acuerdo padres e hijos uso móviles Policía

CONSEJOS DE USO DE DISPOSITIVOS MÓVILES

- Sólo compartir su número de móvil o datos de usuario en Redes Sociales a conocidos reales y de confianza.

- Evitar el uso del móvil para insultos, acoso, sexting y que acudan a un adulto ante un posible ciberacoso o grooming.

- Consultar y pedir autorización paterna antes de descargar aplicaciones y servicios Premium (pago) de las mismas.

- Instalar en los dispositivos herramientas de seguridad y protección así como medidas de control parental.

MÓDULO 2

USO SEGURO DE REDES WIFI

PRECAUCIONES EN EL USO DE REDES WIFI PÚBLICAS

Las redes wifi gratuitas pueden ser de gran utilidad en ciertas ocasiones, pero es necesario que los menores conozcan que son uno de los medios que utilizan los ciberdelincuentes para obtener información una vez que conectamos a ellas.

Des del Oficina de Seguridad del Internauta (OSI), hacen una serie de recomendaciones para que las usemos con precaución.

1. Evitar la conexión automática y eliminar los accesos a redes WIFI una vez finalizado su uso.

2. Evitar realizar compras online o intercambiar información sensible.

3. Comprobar que la red gratuita disponible es la oficial del lugar en el que estamos.

4. Proteger la pantalla del dispositivo de miradas indiscretas.

5. Ser precavidos y mantener actualizados los dispositivos y sus aplicaciones.

6. Siempre que estén disponibles, conectarse a páginas con certificado de seguridad con https://

http://www.osi.es/sites/default/files/actualidad/blog/infografia-como-protegerse-wifi-publica.png

MÓDULO 3

MEDIDAS DE PROTECCIÓN EN EL USO DE DISPOSITIVOS MÓVILES

3.1. NÚMERO DE IDENTIFICACIÓN DEL DISPOSITIVO

Los dispositivos móviles poseen un número de identificación exclusivo para que sea localizable en caso de robo.

Este número se denomina IMEI y es el acrónimo en inglés de “Identidad de Equipo Móvil Internacional”.

Es necesario que guardemos una copia de este número, ya que en caso de robo, se requerirá para poder identificarlo, ya que se ha podido cambiar la tarjeta o estar inoperativo por un tiempo.

Para obtener el código IMEI de un móvil introducimos la combinación *#06# y automáticamente aparecerá en la pantalla del terminal.

Es un número compuesto por 15 dígitos que se corresponderá con el IMEI del teléfono móvil.

También puede localizarse desde la opción Ajustes/ Acerca del dispositivo / Estado / IMEI

3.2. BLOQUEO DE PANTALLA

Para que nuestros dispositivos móviles estén protegidos en caso de extravío o que caigan otras manos, es necesario definir una opción de bloqueo de pantalla para que se active cuando no se esté utilizando el teléfono.

Podremos utilizar varias opciones:

- Dibujar un patrón de desbloqueo.
- Introducir un pin para bloquear.

De esta forma, cada vez que vayamos a utilizar el dispositivo se requerirá el patrón o contraseña de desbloqueo para que podamos acceder.

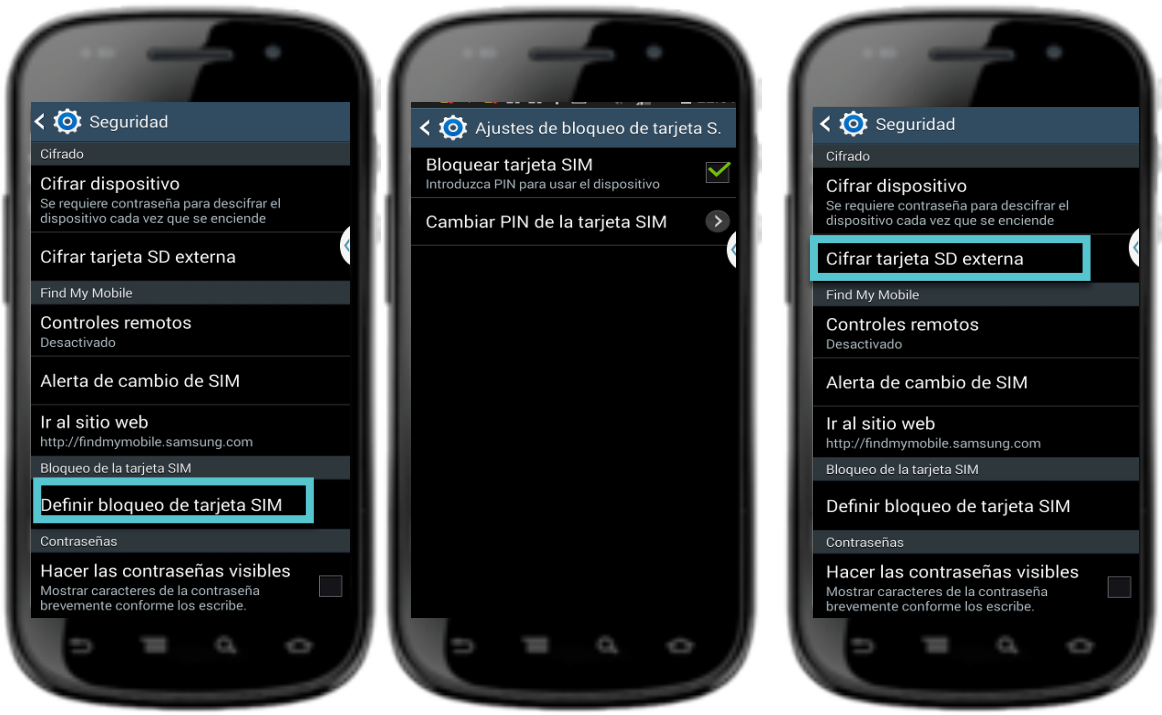
Para configurar esta funcionalidad, accedemos a Ajustes / Seguridad / Cifrar dispositivo.

3.3. BLOQUEO DE LA SIM y SD EXTERNA

Esta función protege el dispositivo para que cada vez que lo encendamos solicite el PIN.

De esta forma, en caso de pérdida o robo, si no conocen el PIN del dispositivo, no podrán acceder a él.

Esta funcionalidad está disponible en: Configuración / Seguridad / Definir bloqueo de tarjeta SIM.



También existe la posibilidad de bloquear la tarjeta SD externa del dispositivo. De esta forma, si esta unidad de almacenamiento es sustraída sólo se podrá acceder a la información que contiene mediante la contraseña que le hemos asignado.

3.4. SISTEMA OPERATIVO SIEMPRE ACTUALIZADO

Al igual que en un ordenador, se hace imprescindible tener el software de estos dispositivos móviles actualizado así como las aplicaciones que tenemos instaladas en los mismos.

Esto evitará posibles amenazas y fallos en la seguridad.

Para comprobar que nuestros dispositivos tienen el sistema operativo actualizado, accedemos a Ajustes / Acerca del teléfono / Actualización de software.

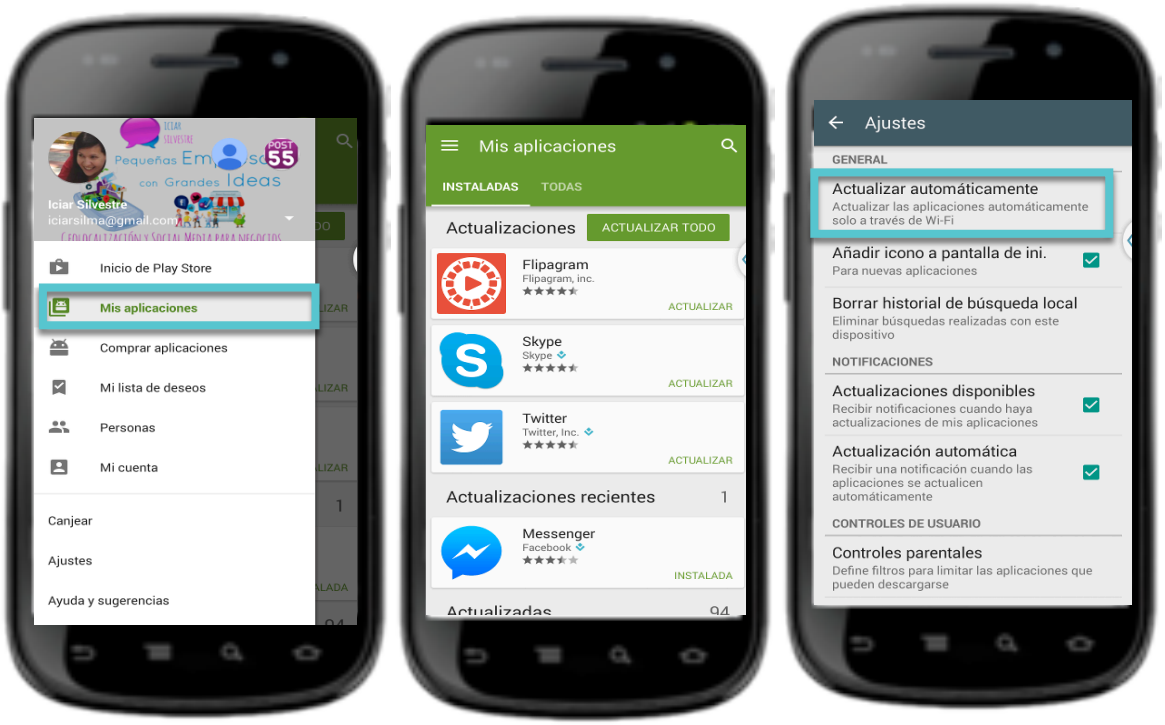
Podemos configurarlo para que las nuevas actualizaciones se instalen de forma automática.

3.5. INSTALACIÓN AUTOMÁTICA DE ACTUALIZACIONES DE APPS

Las aplicaciones también es recomendable actualizarlas para que, además de que se introduzcan nuevas funcionalidades y mejoras, corregir fallos de seguridad.

Para comprobar si las aplicaciones están actualizadas, accedemos a la Google Play y en el menú de “Aplicaciones” veremos aquellas que ya utilizan la última versión de las mismas.

Para cambiar la configuración de las actualizaciones de las aplicaciones accedemos a Google Play / Menú / Ajustes / Notificaciones / Actualizar automáticamente / Actualizar sólo por Wi-Fi (así evitaremos un gasto innecesario de los datos móviles)



3.6. POSIBLES INFECCIONES DE DISPOSITIVOS MÓVILES

El aumento de usuarios con smartphones y tablets, unido a una baja o nula percepción de los problemas de seguridad implícitos a estos dispositivos, hace que sean un objetivo importante de los cibercriminales con dos fines principalmente:

- Espiar qué hacemos con el dispositivo: páginas web que visitamos, servicios que usamos (Twitter, Paypal, banca online), robar nuestras credenciales, fotos y vídeos que realizamos, etc.

- Controlar nuestro dispositivo convirtiéndolo en un "zombi" o bot, sin que nosotros seamos consciente de ello. ¿Y para qué quieren hacer eso? Para envío de spam, infectar otros dispositivos móviles o realizar cualquier otra acción delictiva que se les ocurra desde nuestro móvil.

Existen varios caminos de entrada para que infecten nuestros dispositivos:

- Aplicaciones.
- Ficheros adjuntos en correos, a través de descargas o enlaces publicados en redes sociales.
- Tarjetas de memoria y accesorios extraíbles.
- Enlaces en códigos QR.

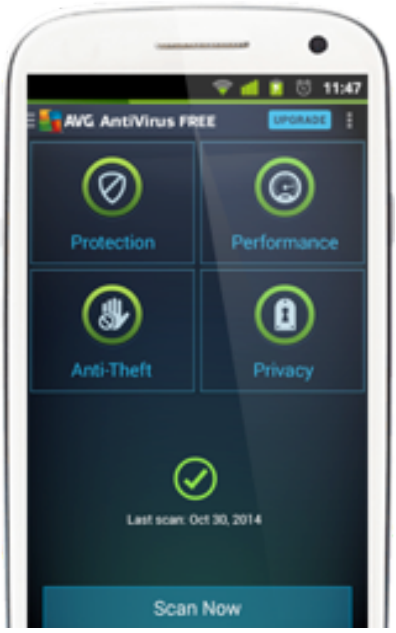
3.7. INSTALACIÓN Y CONFIGURACIÓN DE ANTIVIRUS

Sólo un 32% de los españoles que tienen smartphone tienen un programa de antivirus en el móvil.

Los dispositivos móviles son pequeños ordenadores, y por tanto, es necesario que tomemos medidas de seguridad para que no sean infectados.

Para evitar que nuestros teléfonos y tabletas se infecten de archivos dañinos, podemos instalar como medida de precaución un Antivirus.

Por ejemplo, podemos utilizar la versión gratuita de la aplicación AVG Antivirus Free para que analice las páginas que visitamos a través de estos dispositivos móviles, así como para que verifique si hay algún riesgo en alguna aplicación que nos hayamos descargado o algún archivo que nos hayan enviado a través de correo electrónico o con un enlace de descarga.



Para ello, nos dirigimos a la tienda de aplicaciones y buscamos “AVG Antivirus Free”.

Una vez instalado podremos hacer un rastreo inicial en busca de archivos infectados o alguna amenaza de seguridad en nuestro dispositivo.

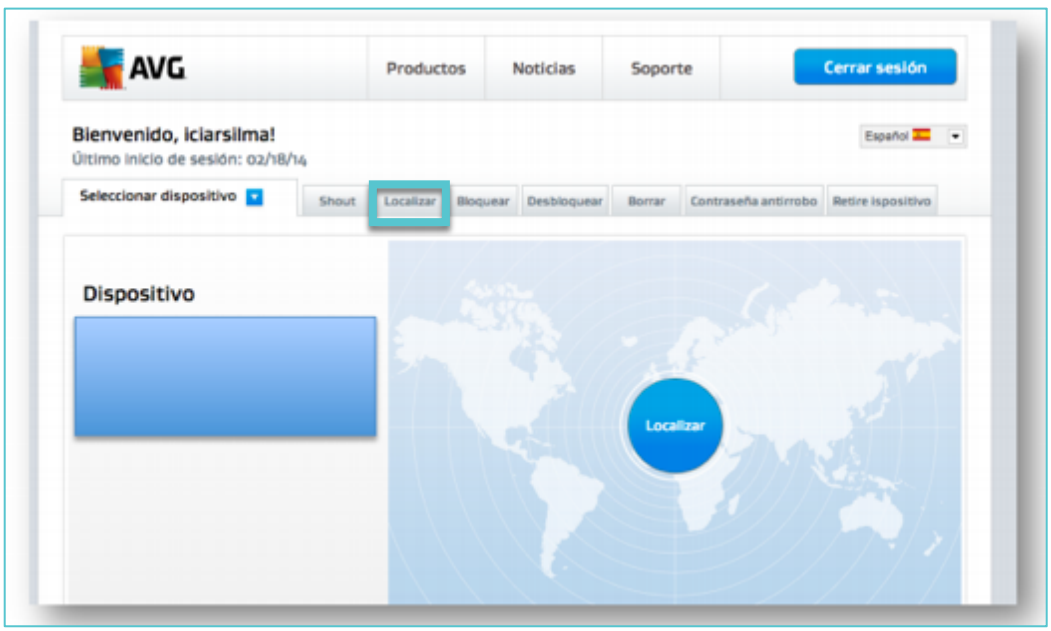
Analizador de aplicaciones
Analizador de Archivos
Analizador de configuración
Navegación segura en Internet

3.7. INSTALACIÓN Y CONFIGURACIÓN DE ANTIVIRUS

Este tipo de aplicaciones ofrecen también la posibilidad de poder localizar el dispositivo a través de una página web.

http://www.avg.com/es-es/antivirus-for-android

De esta forma, el móvil será localizado en Google Maps en caso de robo o extravío.



3.8. LOCALIZACIÓN DEL DISPOSITIVO

Si perdemos el dispositivo Android asociado a nuestra cuenta de Google, el Administrador de dispositivos Android puede ayudarnos a encontrarlo, a bloquearlo o a borrar los datos.

Para ello, accede con tu cuenta de Google a Device Manager y podremos hacerlo sonar, cambia la contraseña de bloqueo remotamente o borra todos los datos almacenados en el dispositivo.

En la página https://support.google.com/accounts/answer/3265955 podremos encontrar toda la información acerca de esta opción.

Activar o desactivar el Administrador de dispositivos Android

Si pierdes tu dispositivo Android, puedes utilizar el Administrador de dispositivos Android:

- **Encontrar tu dispositivo:** utiliza el Administrador de dispositivos Android para mostrar la ubicación de tu dispositivo.
- **Hacer sonar, bloquear o borrar los datos de un dispositivo perdido:** utiliza el Administrador de dispositivos Android para hacer sonar el dispositivo y bloquearlo de forma remota, borrar todo su contenido o añadir un número de teléfono a la pantalla de bloqueo.

Configurar el Administrador de dispositivos Android

Paso 1: Activa o desactiva el Administrador de dispositivos Android

Paso 2: Asegúrate de que el acceso a la ubicación está activado

Paso 3: Comprueba que el Administrador de dispositivos Android pueda localizar tu dispositivo

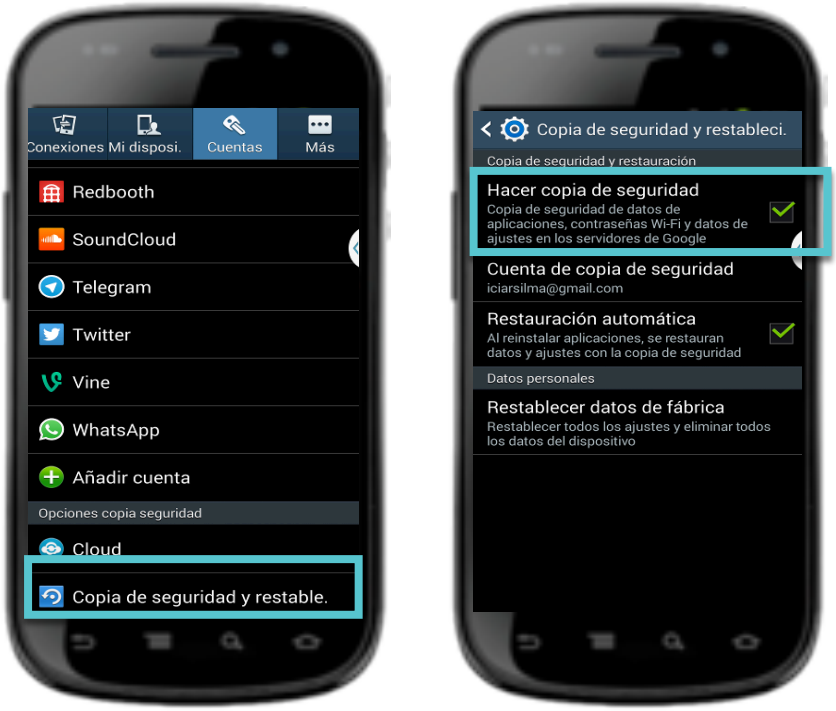
3.9. COPIAS DE SEGURIDAD

Los dispositivos móviles disponen de una opción para hacer una copia de seguridad de todos los datos almacenados en los mismos.

La copia de seguridad estará asociada a una cuenta, por lo que si utilizamos un email de Gmail podremos exportar los datos a la unidad de almacenamiento que nos ofrece de Google Drive.

Podremos hacer la copia de seguridad que quedará almacenada en nuestro dispositivo, pero es necesario que la exportemos a una unidad de almacenamiento externa, ya que si se nos extravía o nos roban el dispositivo, esa copia de seguridad también la perderemos.

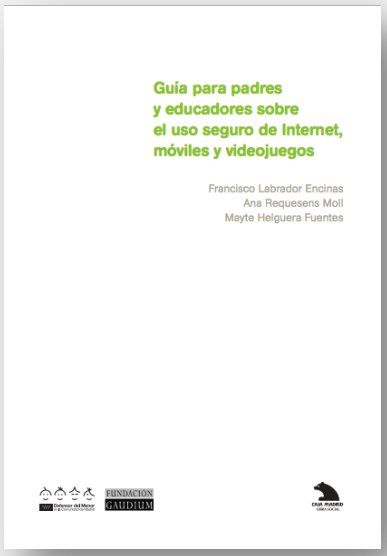
Para hacer la copia de seguridad accedemos a Ajustes / Cuentas / Copia de Seguridad / Hacer copia de seguridad.

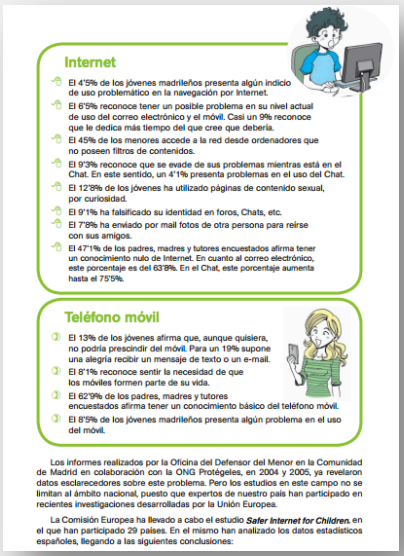


ANEXO

INFORMACIÓN DE INTERÉS

DOCUMENTACIÓN RECOMENDADA





- La Guía para padres y educadores sobre el uso seguro de Internet, móviles y videojuegos ofrece información y recomendaciones para padres, tutores y educadores sobre las precauciones que deben tener los menores en el uso de Internet.

- Incluye información detallada sobre prevención para evitar adicciones a las nuevas tecnologías y recomendaciones para combatir estos problemas si surgieran.

PÁGINA RECOMENDADA

La página Centro de Internet Segura ofrece información actualizada de los posibles peligros que pueden encontrar los menores en Internet.

Posee numerosos recursos para padres, menores, profesores y Centros Educativos de forma gratuita para conocer más acerca de seguridad online.

Aviso Legal