USO SEGURO Dispositivos móviles y MEDIDAS DE PRECAUCIÓN

SEMINARIO ONLINE 2

ÍNDICE

INTRODUCCIÓN

Atendiendo a los datos extraídos del Estudio “Menores de Edad y Conectividad Móvil en España: Tablets y smartphones” elaborado por el Centro de Seguridad en Internet para menores de España: PROTEGELES, en 2014 la inclusión de los teléfonos inteligentes en nuestro país es la mayor de Europa.

Así, mientras la media en países Europeos como Inglaterra, Francia o Alemania es del 57%, en España alcanza el 66%.

Las tabletas adquieren cada vez más fuerza, con unos 7 millones de unidades vendidas en 2013.

Además España es uno de los principales países en utilización de las Redes Sociales, ya que el 93% de los internautas españoles acceden a las mismas.

Pero el estudio desvela que entre los niños y adolescentes hay un claro descenso en la utilización de las redes sociales “clásicas” como Tuenti o Facebook, mientras crece rápidamente las redes sociales a partir de sistemas de mensajería instantánea tipo WhastApp. Por ello, se hace necesario un conocimiento profundo de cómo utilizan los menores este tipo de aplicaciones desde sus dispositivos así como una supervisión familiar de las mismas.

SEGURIDAD

USO RESPONSABLE

PRECAUCIÓN

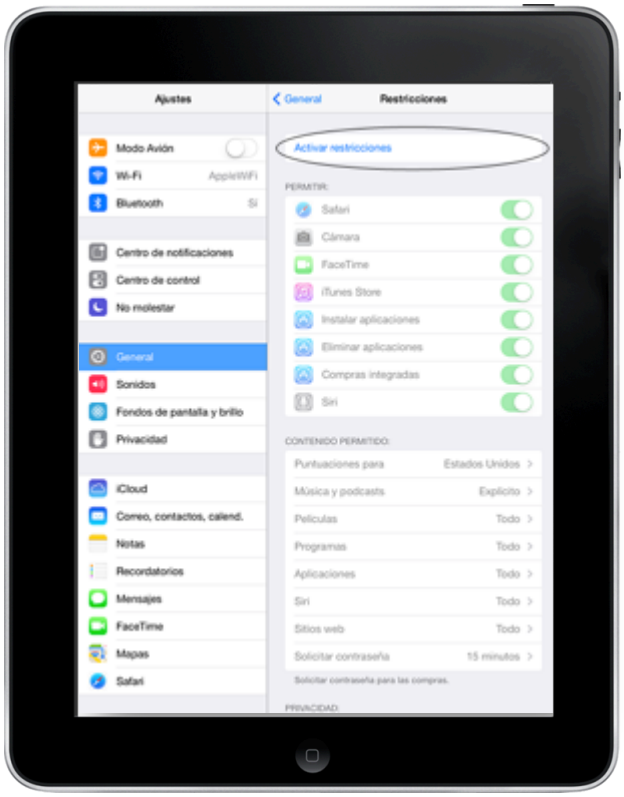
MÓDULO 1

RESTRICCIONES EN DISPOSITIVOS MÓVILES

1.1. RESTRICCIONES EN IPAD

En las tabletas con sistema operativo iOS, los iPAD, podemos configurar una serie de restricciones para que los menores no puedan acceder a ciertas aplicaciones.

Existen aplicaciones específicas en la App Store como Kids Safe Browser With Parental Controls para poder restringir también el acceso a aplicaciones y evitar posibles riesgos.



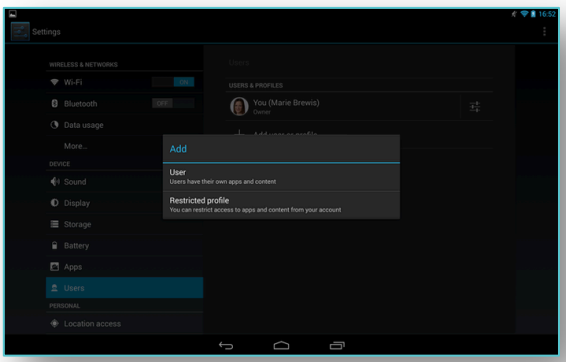
1.2. CONTROL PARENTAL EN ANDROID

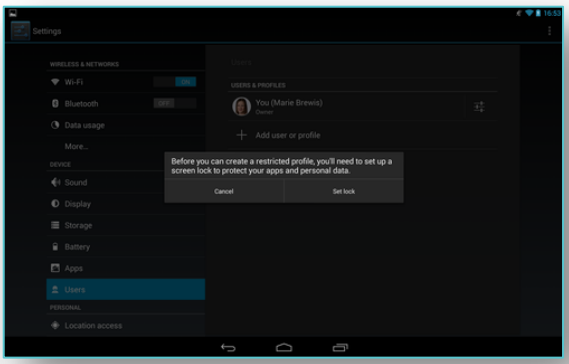
Los niños son cada vez más conocedores de la tecnología en estos días, y hasta un niño se las arreglarán para utilizar su smartphone o tableta.

Las tabletas Android permiten utilizar diferentes perfiles con accesos restringidos.

Para configurar esta opción, podemos seguir los siguientes pasos:

- En la opción de “Configuración” accedemos a “Usuarios” y luego a “Añadir usuario o perfil”.

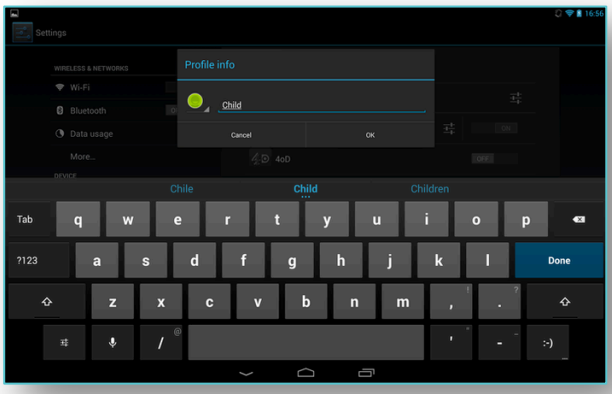


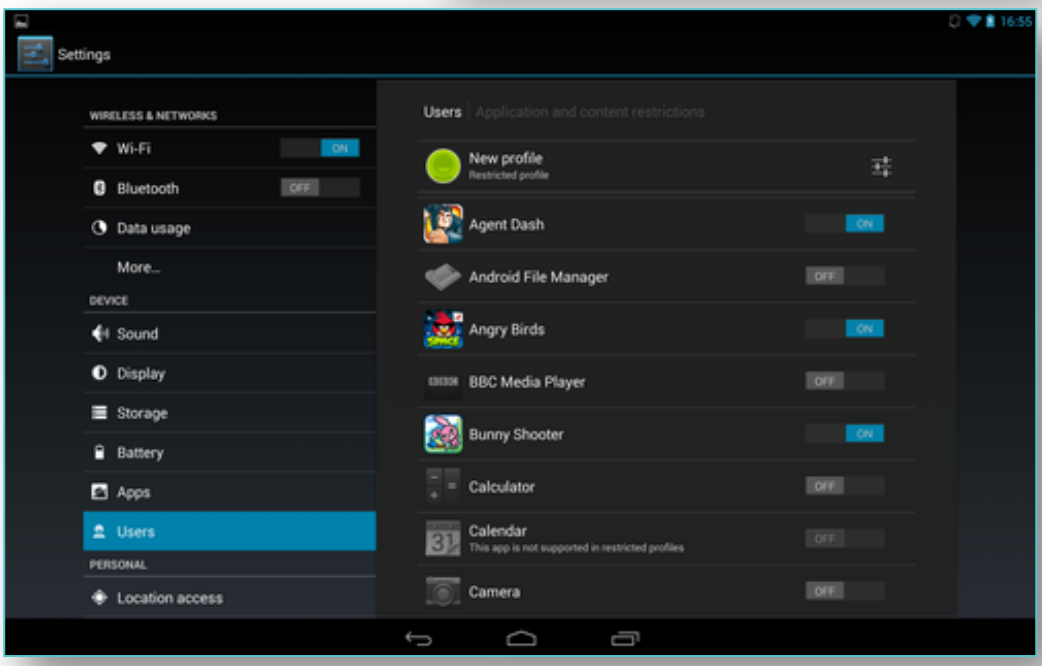


- Haremos clic en el icono de configuración junto al “Nuevo perfil” para darle un nombre.

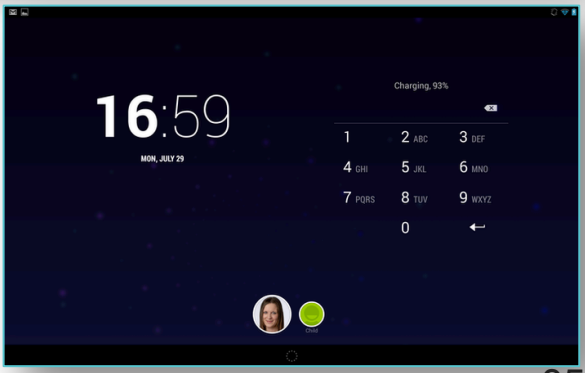
1.2. CONTROL PARENTAL EN ANDROID

- Aparecerá una lista de las aplicaciones instaladas en el dispositivo, con encendido / apagado. A través de la lista que aparece se seleccionará las aplicaciones a las que el niño tendrá acceso.





- De esta forma al encender la tableta podremos elegir el usuario que podrá utilizar el dispositivo en ese momento.



1.3. CONTROL PARENTAL EN VARIOS DISPOSITIVOS

Una de las medidas que padres y tutores tienen disponible para poder hacer un seguimiento y supervisión de la utilización de los dispositivos móviles de los menores a su cargo, es la Aplicación Qustodio.

Con esta aplicación podremos estar al tanto de la actividad de los menores así como poder establecer ciertos criterios de restricción de uso.

MÓDULO 2

USO DE APLICACIONES DE FORMA SEGURA

2.1. UTILIZACIÓN DE WHATSAPP CON SEGURIDAD

Entre los consejos que podemos indicar para un uso seguro y responsable de WhatsApp y hablarlo con los menores, estarían los siguientes:

- No envíes mensajes ofensivos a ningún contacto, se respetuoso y trata con educación a tus contactos. ¡Netiquétate!

- No envíes a través de la aplicación información privada sobre ti: datos bancarios, número PIN del móvil o tus contraseñas de acceso a otros servicios/aplicaciones. No sabes lo que tus contactos podrían hacer con esa información…

- Cuida tu imagen, no envíes fotos ni vídeos tuyos en los que aparezcas en situaciones comprometidas (sexting). En el momento que envías una foto o vídeo a un contacto, pierdes su control para siempre pudiéndote esto ocasionar problemas en tu vida personal, profesional, etc.

- Cuidado con las redes Wi-Fi que utilizas para enviar «whatssApp's». Si no están debidamente protegidas o son redes Wi-Fi públicas, un delincuente o persona con malas intenciones podría capturar las conversaciones que intercambias con tus contactos.

- Atento a los mensajes en cadena, bulos, que circulan a través de WhatsApp, no te creas cualquier mensaje que te envíe un contacto (aunque éste sea de confianza). Contrasta la información, antes de realizar cualquier acción, con otros contactos, páginas web de confianza, etc.

- Antes de abrir un fichero que te han enviado, es recomendable analizarlo con un antivirus para comprobar que no contiene virus.

- Elimina el historial de tus conversaciones para evitar que si alguien accede a tu dispositivo móvil, pueda leerlas y obtener información sobre ti que no deseas.

2.1. UTILIZACIÓN DE WHATSAPP CON SEGURIDAD

Existen muchas estafas que han ido apareciendo con esta aplicación de mensajería como protagonista. Entre ellas:

Se ha identificado en Google Play una aplicación llamada «Activar Llamadas Whatsapp» que utiliza como pretexto la reciente activación del servicio de llamadas de Whatsapp para engañar a los usuarios para que se suscriban a servicios SMS Premium.

Aprovechando la reciente actualización de Whatsapp, están circulando en redes sociales anuncios de una aplicación "WhatsApp Edición ORO" para, supuestamente, mejorar la experiencia de usuario. No obstante, lejos de eso, se subscribe a los usuarios a contenidos que pueden costar hasta 36,25€ al mes.

2.2. OTRAS APPS DE CHAT

Telegram cuenta con el número más bajo de usuarios. La aplicación destaca no sólo por su facilidad de uso (ya que es idéntica a WhatsApp) o por permitir enviar archivos de hasta 1Gb de tamaño, sino especialmente por su seguridad.

Cuenta con un cifrado que la propia compañía califica de “indescifrable” lo que hace muy difícil que terceras personas puedan leer nuestros mensajes aunque los intercepten.

También ofrece la posibilidad de enviar mensajes que se auto eliminan tras un tiempo programado y utilizar un sistema todavía más seguro denominado chat secreto.

Los chats secretos usan cifrado de móvil a móvil de modo que nadie excepto los interlocutores puede leer las conversaciones. Además, permiten la autodestrucción de los mensajes y evitan que éstos puedan ser reenviados. Para asegurarse de que Telegram no tiene acceso a la conversación, ambas personas tienen que comprobar que comparten la misma clave. Para ello se pueden utilizar las “claves visuales”, aunque esto reduce la usabilidad de la aplicación.

Por último, el código de Telegram es abierto y libre, por lo que ya han aparecido múltiples versiones para distintos entornos (Windows, iOS, Android, navegadores web, etc.). Además, estos clientes pueden utilizar los servicios proporcionados por los centros de datos de Telegram libremente.

2.2. OTRAS APPS DE CHAT

Snapchat es una app utilizada principalmente por el público más joven debido a la opción de edición de imágenes y vídeos con autodestrucción. Pero es necesario que los menores sean conscientes de su seguridad y conocer más sobre las publicaciones que en ella comparte.

Snapchat permite enviar imágenes y vídeos que solo serán reproducibles durante unos segundos. La aplicación muestra los estados de recepción: permite saber si un a imagen ha sido enviada, abierta y el tiempo restante de visualización.

Asociar la cuenta al número de teléfono es opcional, así que se deben añadir a los usuarios para que puedan ver los snaps del usuario. Además es posible saber si la persona receptora ha hecho captura de pantalla. Se puede decidir si enviar una foto a una persona o dejarlo como una “historia”. Entonces, los usuarios pueden leerla durante 24h.

También es posible establecer si el acceso a las historias de Snapchat se permite a todo el mundo o solo a tus contactos. Permite bloquear todos aquellos usuarios que quieras.

https://www.youtube.com/watch?v=xKc0hnznhSg

2.3. APPS CON FUNCIÓN DE GEOLOCALIZACIÓN

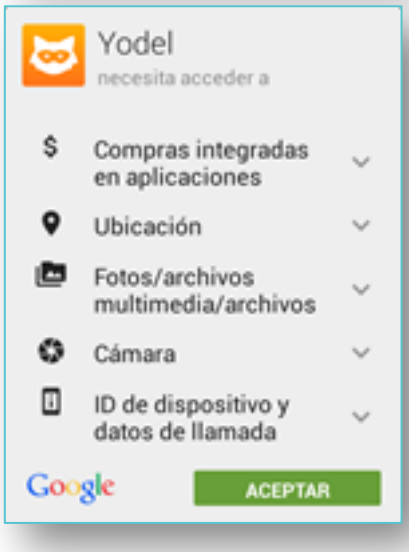
Muchas apps de redes sociales tienen disponible la opción de "geolocalización".

Es necesario que hablemos con los menores sobre esta función para que sean conscientes de las repercusiones que tiene en tema de seguridad y privacidad en la Red sobre, por ejemplo, imágenes que incluyan datos e información sobre el lugar exacto donde nos encontramos en cada momento.

2.3. APPS CON FUNCIÓN DE GEOLOCALIZACIÓN

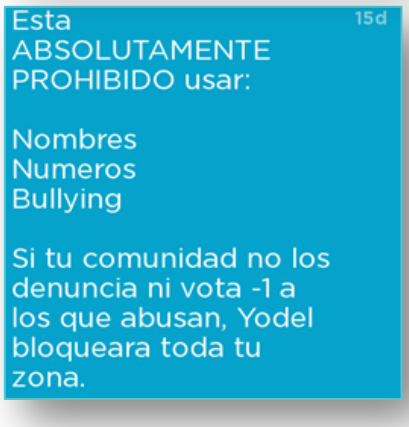
Yodel es una aplicación que utiliza como principal herramienta el GPS de los dispositivos móviles.

En la Google Play y en la App Store la definen como una “comunidad online que te muestra lo que está pasando en tu área en tiempo real de forma anónima”. En un tablón de anuncios se pone en común para los usuarios lo que está ocurriendo en un radio de 10 km, y cuya principal novedad que no requiere un registro como los que estamos habituados.



Para utilizarla se requiere un correo electrónico/ usuario/número de teléfono, por lo que muchos usuarios piensan que es anónima.

La aplicación permite establecer conversaciones, votar positivo o negativo a los mensajes de otros usuarios, etc.



Es una app que está produciendo cierta preocupación entre padres y profesores, ya que se están detectando problemas de privacidad, ciberbullying, acoso, difusión de contenidos que podrían atentar contra el honor, derecho a la propia imagen, etc; por parte de usuarios malintencionados.

Cuando nos damos de alta aparece unas advertencias de uso y varios mensajes con los “Yodel-Mandamientos” como guía de buen uso.

Entre las funcionalidades, almacena los siguientes datos, por los que se puede intuir que no es totalmente anónima.

- Mis Yodels.
- Mis respuestas.
- Mis votos.
- Mis mejores Yodels.
- Localización actual.

MÓDULO 3

RECOMENDACIONES FINALES DEL USO INTELIGENTE DE DISPOSITIVOS MÓVILES

RECOMENDACIONES

Recopilando todo lo que hemos comentado sobre el buen uso de los dispositivos móviles, a continuación destacamos algunas de las recomendaciones que hacen desde el INCIBE (Instituto Nacional de Ciberseguridad):

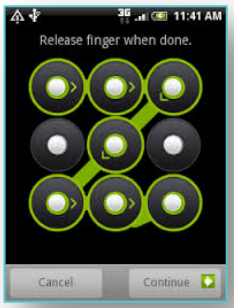
No perder nunca de vista el teléfono en lugares públicos y no prestarlo a personas extrañas.

En caso de intento de robo, preservar la integridad física y renunciar al móvil.

Activar el código PIN (código personal que permite, o impide, acceder a la tarjeta SIM del tléfono) y mantener en lugar seguro el código PUK (código de seguridad que permite desbloquear el teléfono si se ha errado en la introducción de PIN en tres ocasiones.

Activar la opción de bloqueo del terminal con solicitud de contraseña para desbloquearlo.

Aunque el teléfono no permita hacer llamadas telefónicas, puede permitir el acceso a los datos que contiene (información personal).



RECOMENDACIONES

Utilizar siempre contraseñas robustas para proteger el acceso a sus conexiones.

Evitar datos que podrían ser fáciles de conocer como la fecha de nacimiento, matrículas, etc.

Vigilar el consumo en la tarifa telefónica e informarse, de inmediato, ante cualquier anomalía.

En el caso de los menores puede ser conveniente utilizar el sistema de tarjetas prepago.

No abrir correos electrónicos, ni aceptar archivos, si no se conoce al remitente.

Tampoco contestar nunca a SMS desconocidos y tener instalado siempre software original.

RECOMENDACIONES

No dejar encendido el Bluetooth encendido si no se está utilizando, ya que esta tecnología podría que servir a los ciberdelincuentes si no se utiliza con seguridad.

Acostumbrar a los menores a pedir permiso antes de fotografiar a amigos o conocidos en lugares como colegios, piscinas, etc; ya que en lugares públicos está prohibido y podríamos incluso estar infringiendo la Ley.

No contestar nunca a SMS de contenido amenazante. Si se perciben amenazas a través del móvil es aconsejable anotar la hora de la llamada, guardar el mensaje y ponerlo en conocimiento de la dirección del centro escolar y de la Policía.

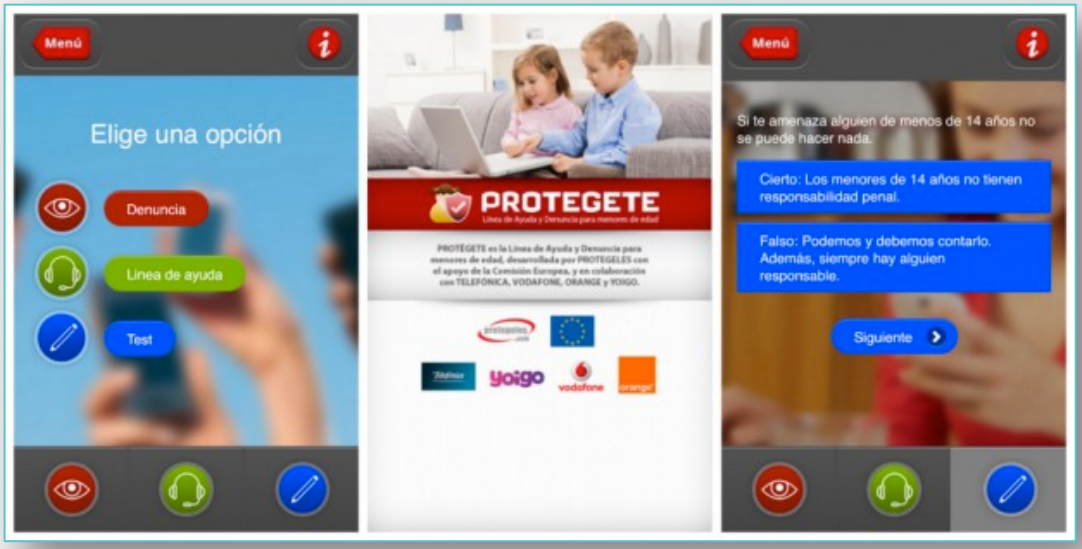
RECOMENDACIONES

Comprobar periódicamente los números de teléfono almacenados en los teléfonos móviles de los menores y hablar con ellos con frecuencia sobre las personas con las que mantienen contacto a través de estos dispositivos.

ANEXO

INFORMACIÓN ÚTIL

APLICACIÓN RECOMENDADA



- La aplicación PROTÉGETE supone una herramienta anti-acoso que puede ser utilizada por los menores.

- Esta herramienta ofrece opciones como la denuncia de forma anónima de contenidos ilegales o inadecuados que se encuentran en Internet.

- Tiene un sistema para pedir ayuda en situaciones de acoso en Internet (ciberbuying), de acoso sexual hacia menores (grooming), casos de usurpaciones de identidad y otro tipo de problemas relacionados con Internet y las Nuevas Tecnologías.

- Permite evaluar el nivel de conocimiento de los menores sobre seguridad y uso responsable de Internet y las Tecnologías de la Información y la Comunicación.

La aplicación puede descargarse de forma gratuita desde la web de protegeles.com

ACTIVIDAD PARA HACER EN FAMILIA

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

- En la web del Instituto Nacional de Ciberseguridad (INCIBE) podemos encontrar amplia información sobre medidas de protección y prevención de los equipos informáticos que utilicemos.
- Además, ofrece noticias actualizadas sobre fraudes y peligros existentes en la Red para estar informados y estar prevenidos ante ellos tomando las medidas oportunas.
- También dispone de un servicio de asistencia y soporte desde el cual se puede solicitar asistencia ante un incidente de seguridad o realizar consultas sobre legislación vigente en materia de tecnologías de la información.

Aviso Legal