

La presente guía es un documento orientativo con la única finalidad de fomentar el uso responsable de las nuevas tecnologías en los centros escolares y sin valor vinculante alguno.

Guía de recomendaciones para un uso seguro de Whats App

Los riesgos de Whats App

1.- DEFINICIÓN DE WHATS APP.

Servicio de mensajería ejecutado desde el teléfono móvil muy popular entre adultos y menores debido a su coste además de a su sencillez de instalación, configuración y uso.

2.- MOTIVO DE LA GUÍA.

Que los padres, educadores y alumnos conozcan no sólo las ventajas de su uso:

- **Los riesgos que comporta** por la gran cantidad de información privada que se gestiona y a la que se accede desde esta aplicación.
- **Las recomendaciones de seguridad** para prevenir los riesgos

3.- ¿QUÉ RIESGOS TIENEN ESTE SERVICIO?

A) Riesgos para la privacidad

El más importante es la privacidad de las comunicaciones que hace posible la suplantación de la identidad.

Para enviar mensajes, este servicio no pide un nombre de usuario y contraseña, sino que utiliza el propio número del teléfono y una clave que genera en función del móvil

B) Riesgos en caso de pérdida o robo.

B.1. Suplantación. Cualquier persona puede enviar mensajes desde cualquier móvil que caiga en sus manos si éste no está protegido (p. ej.: está encendido y no pide clave o patrón de acceso o está apagado y no tiene PIN). Es decir, se puede hacer pasar por nosotros en «conversaciones» con otros usuarios del WhatsApp.

Si ocurre de forma esporádica, podríamos hablar de una suplantación o apropiación de identidad, si es continua, (robo de móvil) es un robo de identidad.

B.2. Robo de información. A través de Whatsapp se accede a gran cantidad de información:

- *personal, privada e íntima, - familiar, - de amigos, - Fotos y videos*

Que tenemos en nuestra agenda, en los chats y conversaciones y que es posible volcar con un simple click a una tarjeta u ordenador.

4. ¿QUÉ HAY QUE HACER PARA PROTEGERNOS?

A) En caso de pérdida o robo

- DENUNCIARLO A LA POLICÍA

- COMUNICARLO AL OPERADOR. La desactivación de la tarjeta SIM no desactiva whatsapp, por lo que hay que solicitar otra tarjeta urgente y volver a activar la aplicación para que, de esa manera, WhatsApp anule el registro del móvil robado.

B) ¿Cómo evitar la apropiación o robo de identidad con el móvil?

La forma más sencilla de prevenir que alguien utilice nuestro móvil (WhatsApp, llamadas, SMS, ver fotos o vídeos...) es utilizar el bloqueo del terminal, todos los dispositivos lo tienen, y es efectivo por que no depende de la tarjeta SIM.

Para activar el bloqueo de móvil, en cada sistema se hace de una forma distinta, en los más importantes:

- **Android:** La opción está en Ajustes>Ubicación y seguridad>Bloqueo de pantalla. Se puede seleccionar: patrón, PIN de bloqueo y contraseña.
- **IOS (Apple):** La opción está en Ajustes>General>Bloqueo con código.
- **BlackBerry:** La opción para bloquear el terminal está en Menú>Opciones>Contraseña
- **Windows Mobile:** La opción se activa en Inicio>Configuración>Bloqueo.
- **Symbian:** Herramientas>Ajustes>Seguridad>periodo de bloqueo auto.

Por último os aconsejamos actualizar la aplicación WhatsApp, ya que la última versión cifra y encripta los mensajes, y poner contraseña para acceder a la información de la tarjeta SD en caso de que la uséis con finalidad de almacenamiento.

La presente guía es un documento orientativo con la única finalidad de fomentar el uso responsable de las nuevas tecnologías en los centros escolares y sin valor vinculante alguno.