Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

Mediación Parental

Disponibilidad. La familia siempre estará a su disposición. Evitar reacciones exageradas o culpabilizarle, generará más confianza.

Fomentar las habilidades sociales y el pensamiento crítico. La interiorización de un espíritu crítico que les ayude a sopesar todas sus actuaciones y decisiones. La **autoestima, la asertividad y la empatía** son habilidades sociales positivas que le ayudarán a enfrentarse de manera adecuada a los conflictos.

Supervisión y diálogo. Si optamos por el uso de herramientas de control parental, conviene hablar con el menor de la instalación de estas herramientas y las razones de utilizarlas.

Escuchar y orientar. La comunicación es un canal que debe mantenerse abierto en las dos direcciones, por ello es necesario escucharles, saber lo que piensan, lo que hacen y cómo se relacionan en Internet. NO prejuzgar y centrarse en las actitudes que se considera necesario mejorar.

Promover el equilibrio en el uso de las nuevas tecnologías

Evitar la conexión por aburrimiento y hábitos de conexión que interrumpan otras actividades

Transmitir la idea de que **Internet es un espacio público**, en el que cualquiera puede ver lo que haces, compartes o publicas

Fomentar la autoconfianza y mantener hábitos saludables fuera de Internet. (Deporte, actividades al aire libre, leer o pasar tiempo con sus amigos) básico para **impedir que Internet sea la única opción de ocio para ellos**

Gestionar sus emociones y estados de ánimo es importante, para evitar que Internet sirva como refugio a la hora de resolver sus problemas.

Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

¿Cómo reaccionar en caso de conflicto?

Responder con calma. Estamos para apoyarles y ayudarles a resolver el problema. Debemos enfocarnos a buscar una solución y proteger al menor.

Contacto con los difusores. Contactar, si es posible, con quienes estén difundiendo los contenidos e incluso con quienes los hayan recibido para evitar que se sigan enviando y pedir su eliminación. Asimismo, contactar con el centro educativo puede ser de utilidad, ya que pueden colaborar con asesoramiento y concienciación.

Reporte al proveedor de servicios. Para que los contenidos se eliminen en muchos casos es necesario comunicarse con el proveedor de servicio (Instagram, Facebook, Twitter, etc.) alertándoles sobre el caso, limita en buena medida su difusión.

Denuncia. Sobre todo en casos de **extorsión y grooming**. En estos casos, será necesario hacer capturas de pantalla y guardar todas las pruebas.

NUNCA aceptar un chantaje. Si nos encontramos ante un agresor que tiene (o dice tener) alguna información sensible en su poder, nunca debemos ceder a la manipulación, ya que empeorará la situación.

Apoyo psicológico. Las consecuencias derivadas por este tipo de prácticas son graves, y el menor puede necesitar apoyo psicológico y emocional. El centro de salud y su centro educativo pueden ofrecernos orientación si es necesario

MEDIDAS QUE PROTEGEN

Opciones de privacidad. Configurarlas adecuadamente es imprescindible en cada aplicación o servicio que utilicen los menores

Opciones de seguridad. Hoy en día cualquier servicio (redes sociales, servicios online, etc.) o dispositivos (ordenadores, tablets y teléfonos móviles) contiene mucha información privada que debe protegerse. El uso correcto de **contraseñas robustas**, **doble verificación**, **bloqueo de pantalla, preguntas de seguridad y otras opciones de acceso es esencial para limitar el acceso**.

Control de contactos y amistades. Es habitual que los menores añadan en sus redes sociales a personas que realmente no conocen, con lo que su información acaba en manos de personas totalmente extrañas. **Promover una lista de contactos segura**, para que puedan controlar con quién comparte la información.

Sincronización. Muchas aplicaciones conectan nuestra cuenta de usuario con otras aplicaciones (como por ejemplo, para tuitear automáticamente las fotos de Instagram). Debemos **revisar los permisos de privacidad de cada aplicación**, para evitar publicar información no deseada.

Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

Uso de equipos públicos. **EVITAR SU USO** si se va a gestionar información sensible o privada. No obstante, de hacerlo, se recomienda utilizar la opción de **navegación privada** del navegador, no guardar las contraseñas y cerrar sesión de los servicios al finalizar para evitar que cualquiera que utilice el equipo a continuación pueda acceder a nuestro correo electrónico, redes sociales, banca online, etc.

Construir contraseñas robustas y distintas en cada página. Al menos con 8 caracteres, combinando mayúsculas, minúsculas, números y símbolos. Sin incluir palabras reales, ni información personal (nombres, DNI, teléfono, fecha de nacimiento…), ni letras o números consecutivos (abc, 123). Cambiarlas con cierta frecuencia.

Usuarios limitados. Crea para tus hijos una cuenta de usuario estándar (en lugar de utilizar la de administrador).

Bloquea el equipo, **cierra sesión**. Al alejarse del ordenador, aunque sea un momento, bloquéalo **(Win+L)** para que nadie pueda acceder a tu información o se haga pasar por ti en el correo electrónico o las redes sociales. En móviles y tablets configura un patrón de desbloqueo, o mejor un pin o una contraseña.

Mantén actualizado el sistema y todos sus programas, aplicaciones, plugins y complementos.

Instala un **antivirus**. También en móviles y tablets. **Mantenlo actualizado**. Analiza el sistema de vez en cuando. Analiza los archivos que recibas por correo, o descargues de Internet, de una memoria USB o una tarjeta de memoria (como las de los móviles y cámaras digitales). **(https://www.virustotal.com/gui/home/upload)**

Piensa antes de instalar. Descarga aplicaciones **sólo desde fuentes oficiales** (Google Play en Android, App Store en iOS). Comprueba que lo que vas a instalar es lo que necesitas, que no es una copia falsa o pirata (puede llevar virus). Comprueba el desarrollador (¿es uno destacado?), cuántas descargas y comentarios tiene, los permisos que pide.

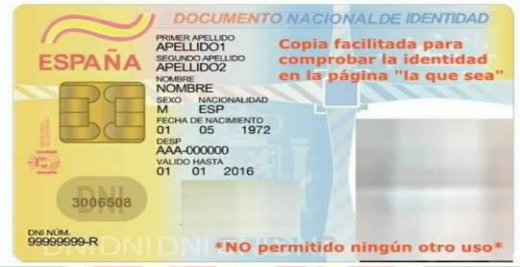
Realiza copias de seguridad periódicamente. Tanto del sistema, como de tu información (contactos, archivos, imágenes, etc.).

Controla tus conexiones. Protege tu WiFi con cifrado WPA2 y cambia las claves por defecto del router de casa. **Evita conectarte a redes WiFi públicas. Desactiva WiFi, Bluetooth y NFC cuando no los necesites.**

Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

CIBERCONSEJOS@ -Evita ser víctima de las ciberestafas-

NO ENVIAR COPIA DE NUESTRO DNI A NADIE ni por WhatsApp, ni por correo electrónico, ni en cualquier otra plataforma. Pero si no tienes más remedio protégelo de la siguiente manera: difuminando firma y fotografía y añadiendo los textos que aparecen en el ejemplo según el fin para el que sea.



DESCONFÍA de los mensajes pidiendo dinero, ingresos, Bizum por whatsapp de un FAMILIAR o amigo (pueden haberle robado la cuenta whatsapp). **CONTRASTAR LA INFORMACIÓN** llamándolo por teléfono y **comprueba esa URGENCIA**(si es urgente te llamará).

USAR TARJETAS VIRTUALES/MONEDERO JAMÁS vincular una tarjeta de crédito o débito a una web o aplicaciones y tampoco realizar compras por Internet con esos tipos de tarjetas. **UTILIZAR LAS TARJETAS VIRTUALES.**

NO CARGAR EL MÓVIL EN ESTACIONES DE CARGA PÚBLICAS (Aeropuertos, autobuses, cafeterias, etc), podrías ser victima del JUICE-JACKING (robar datos del dispositivo).

Hacer caso omiso a los correos @ y sms de ENTIDADES BANCARIAS, CORREOS, HACIENDA, SEGURIDAD SOCIAL, EMPRESAS O DIFERENTES ORGANISMOS OFICIALES. **NO PINCHAR EN SUS ENLACES Y BORRARLO DE NUESTROS DISPOSITIVOS.**

Si eres usuari@ de portales de compraventa tipo MILANUNCIOS O WALLAPOP, cuando vayas a finalizar la compra, MANTENTE ALERTA, pueden que te engañen diciéndote que te dan una señal por BIZUM, solicitándote dinero en vez de enviártelo. En otras ocasiones te envian un enlace para pagarte o te solicitan tu número de tarjeta bancaria para pagarte (Recordemos que a una tarjeta nunca le llegará una transferencia bancaria).

Ante cualquier llamada que recibamos en nuestro teléfono de (BANCOS, ASEGURADORAS, COMPAÑIAS DE LUZ, GAS, ETC) **NO facilitar ningún tipo de datos personales,** ante cualquier duda acudamos a una oficina física.

DESCONFIAR de los precios bajos en cualquier tipo de página web antes de realizar un pago.

NO instalar aplicaciones desde webs o google, ÚNICA Y EXCLUSIVAMENTE desde STORE.

Mantener actualizado un antivirus en todos los dispositivos incluido teléfonos móviles.

ANTE TODO, SENTIDO COMÚN Y BUENAS PRÁCTICAS

Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

Enlaces de interés con recursos e información para un uso seguro y responsable de los menores frente a la Ciberdelincuencia.

https://www.incibe.es/

https://www.is4k.es/

https://www.anar.org/?gclid=CjwKCAjwu_mSBhAYEiwA5BBmf1aa5ycWNgW3KdGIyLNL9iCgyQTl9aEIOzAsdW6XgsDCsmz2g3apSRoCACAQAvD_BwE

https://intef.es/aseguratic/

https://www.pantallasamigas.net/

Plan Director para la Convivencia y Mejora de la Seguridad en los Centros Educativos y sus Entornos

Oficina de Seguridad del Internauta

https://www.osi.es/es

OEDI Observatorio Español de Delitos Informáticos

https://oedi.es/

G.D.T.

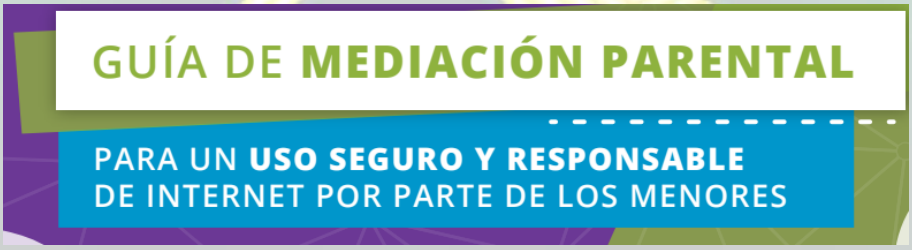
POLICÍA NACIONAL

https://www.gdt.guardiacivil.es/webgdt/home_alerta.php https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php

is4k INTERNET SEGURA FORKiDS

HERRAMIENTAS DE CONTROL PARENTAL

https://www.is4k.es/de-utilidad/herramientas



https://www.is4k.es/sites/default/files/contenidos/materiales/Campanas/is4k-guiamediacionparental.pdf

#CanalPrioritario

https://www.aepd.es/es/canalprioritario

WhatsApp *(900 116 117) y* ***Telegram*** *(@INCIBE017) o también a través del formulario web.*

Horario de servicio

De 9:00 a 21:00 horas durante todos los días del año

(Incluidos sábados, domingos y festivos)

GRATUITO Y CONFIDENCIAL