CIBER EXPERT@

FORMACIÓN EN EL USO SEGURO DE INTERNET

SÉ INTELIGENTE, CONVIÉRTETE EN CIBEREXPERT@

Mediación parental

www.ciberexperto.org

seguridadescolar@policia.es

organiza

Policía Nacional

apoya

Telefónica

colabora

ciber voluntarios .org

MEDIACIÓN PARENTAL

OBJETIVOS DEL TEMA

Para favorecer el uso seguro de las TIC es necesario que el menor cuente con el apoyo de los adultos tanto para proporcionarle información como para ponerle límites en el uso de las tecnologías de la información y la comunicación.

El deber de los adultos es promover la prevención a través del uso responsable de las TIC y prestarle el apoyo necesario cuando se encuentre en dificultades.

El objetivo de este tema es transmitir nociones básicas de la mediación y el control parental, además de ofrecer consejos prácticos para proteger la privacidad del menor a la hora de usar diferentes aplicaciones y servicios online.

- Conceptos.
- Niveles de actuación.
- Estilos de mediación.
- Normas esenciales.
- Herramientas.
- Como reaccionar ante un incidente.

MEDIACIÓN PARENTAL

¿Qué es?

La Mediación parental: Proceso de acompañamiento de los responsables de la educación digital del menor en su formación. Se educa en un uso seguro y responsable de las TIC.

El Control parental: Herramienta o programa tecnológico que permite a familiares y educadores, controlar y/o limitar el uso que un menor hace de internet y de los dispositivos electrónicos que utiliza.

Niveles de capacitación

- **Capacitación tecnológica**: posibilitar en los menores la adquisición de conocimientos, habilidades y actitudes, que les permitan una relación segura y respetuosa con la red.

- **Capacitación conductual**: guiar a los menores, para que hagan un uso de las TIC empático y respetuoso, y teniendo en cuenta reglas básicas de civismo y respeto. (Netiqueta).

Con los dos puntos anteriores, también se crean vínculos que propiciarán que en el futuro recurran a los adultos de su entorno si se enfrentan a un problema de esta índole.

- **Herramientas y recursos**: Permiten controlar y/o limitar el uso de internet o un dispositivo. Ayudan al adulto a guiar, educar y formar al menor en el uso de las TIC, prevenir riesgos y solucionar los incidentes que se produzcan.

Tipos de mediación

Así actuamos los adultos…

- **Imperativo**:
  - Imposición de gran cantidad de normas.
  - Falta de diálogo y comprensión con el menor.
  - Escasa empatía hacia el menor.
  - Se advierte del peligro, pero sin informarles de los riesgos que entrañan un uso inadecuado de las TIC.
  - No hay educación conductual, solo prohibición.

"Tienes que borrar el Snapchat de tu móvil, porque yo te lo digo".

- **Consentidor (lo contrario al anterior):**
  - Ausencia de normas básicas o pocas y muy laxas.
  - Evitan enfrentamientos con los menores.
  - El menor explora en internet bajo su propio criterio.
  - Dejan la educación digital en manos de educadores, amigos, etc.

"Sí, claro que te compramos un móvil, con una cámara mejor para que puedas grabar vídeos".

- **Pasivo:**
  - Ausencia total de normas y límites en el uso de las TIC. Falta de implicación en la educación digital de los hijos.
  - Escasa o nula comunicación con los hijos.
  - Se ignoran y por lo tanto no se informa de los posibles riesgos en el uso de internet, ni se sabe actuar ante situaciones de riesgo.
  - Puede imponer castigos desmesurados sin justificación.

Nunca controlan el acceso a internet, pero de repente un día dicen: "Esta semana te quedas sin internet".

- **Tolerante:**
  - La educación se basa en el ejemplo de los educadores.
  - Normas y límites claros, razonados con sus hijos.

- Afecto y comunicación, educan en la progresiva autonomía del menor, según su madurez.
- Se enseña a identificar los riesgos y a cómo protegerse de ellos.
- Usan herramientas de control parental.
- En definitiva, se establecen pautas para la supervisión, acompañamiento y orientación de los menores en el mundo digital.

"Vamos a acordar los horarios del uso del ordenador, de tal manera que tengas tiempo para hacer los deberes y para divertirte, pero sin que pases demasiado tiempo ante la pantalla, ¿qué te parece?"

<u>...Y así responden los menores</u>

- **Ante educadores imperativos**:
  - Las normas no están interiorizadas, no entienden su porqué y por eso obedecen solo en presencia de los padres.
  - Falta de autocontrol, siempre son los padres quienes les establecen los límites.
  - Buscan y generan contenido inapropiado, no tienen criterio para decidir que es adecuado o no.
  - Baja autoestima y habilidades sociales.
  - No confían en los adultos de su entorno ante dudas o problemas.

- **Ante educadores consentidores**:
  - Ausencia de límites y normas, el menor está acostumbrado a hacer lo que quiere.
  - Intolerancia al intento de establecimiento de normas básicas.
  - Navegan de manera arriesgada, no tienen conciencia de peligros porque nadie les ha explicado cuáles son y en qué consisten los mismos.
  - Susceptibles de hacer un uso abusivo de las TIC y caer en la adicción a éstas.

- **Ante educadores pasivos**:
  - De ningún modo asumen normas o límites.

- Ausencia de empatía con el resto de internautas.
- Vulnerables a los conflictos sociales y personales, con gran propensión a involucrarse en situaciones de *ciberbullying*.
- Desconocen los riesgos y recomendaciones, por lo que pueden sufrirlos con mayor asiduidad.
- Falta de confianza en los adultos de su entorno ante situaciones problemáticas.

- **Ante educadores tolerantes**:
  - Empatizan y tienen una buena competencia digital y social.
  - Conocen los riesgos y los previenen de manera cada vez más autónoma.
  - Son responsables, usan las TIC de forma adecuada y segura.
  - Siguen las normas porque entienden su utilidad.
  - Gracias a una relación de confianza, acuden a los adultos de su entorno ante las dudas o dificultades con los que puedan encontrase.

Herramientas

El control parental es una herramienta útil para la seguridad de los menores. Sin embargo la herramienta más efectiva siempre **será hablar con los menores y darles formación e información** acerca de la vida online; debemos ser, con nuestro ejemplo, la mejor herramienta para nuestros niños y jóvenes.

Opciones que ofrecen los programas de control parental:

- En las páginas web existen una serie de etiquetas que clasifican el contenido de la misma. En función de estas etiquetas ciertos controles parentales pueden **bloquear el acceso a determinadas páginas web** en función de su etiquetado.

- Bloquear ciertos **programas y aplicaciones** (por ejemplo, juegos demasiado violentos).

- Controlar **el horario y las horas** que nuestros hijos pueden usar el ordenador y estar conectados a internet. Permite que el menor no se conecte cuando se encuentre a solas.

- **Monitorización** de las acciones que nuestros hijos realizan con el ordenador. De este modo podemos registrar las páginas web que visitan, el tiempo que dedican a cada una de las páginas que visitan, ver sus hábitos de navegación, etc.

- ***Keyloggers*** guardan las pulsaciones del teclado (información sobre todo el texto que se ha tecleado).

- Bloquear la **información que sale** del dispositivo (datos privados en los formularios e impedir las compras por internet).

- Existen **navegadores infantiles** con un diseño atractivo y contenido apropiado en función de la edad (3-12 años). Pueden ser gratuitas o de pago.

- La utilización de **buscadores infantiles** utilizan filtros para excluir de los resultados de la búsqueda la información inapropiada.

Ejemplos de herramientas

Qustodio es una aplicación gratuita de control parental en internet (existen algunos problemas de incompatibilidad con iPhone):

- Se instala en aquellos dispositivos que se quieran gestionar.

- Los padres no necesitan tener la aplicación instalada en el dispositivo para poder consultar los datos, ya que se puede acceder desde cualquier navegador.

- **Funcionalidades**: bloqueo de pornografía, seguimiento en redes sociales, límites de tiempo, seguimiento de ubicación, botón de pánico, control de mensajes de texto y llamadas, bloqueo de juegos y aplicaciones.

Facebook

En el margen superior derecho de la aplicación se encuentra un icono en forma de candado, donde podremos revisar de forma sencilla la privacidad del perfil en **"comprobación rápida de privacidad":**

1. Es importante revisar qué público tendrá acceso a la información. Lo más recomendable es **compartir información solo con personas que conocemos**, y si es posible, tenerlos clasificados por grupos.

2. El siguiente paso es decidir **qué aplicaciones queremos que tengan acceso al perfil**, ya que muchas podrían publicar información en nombre del usuario, por lo que es fundamental que se lean y asignen detenidamente los controles de permisos.

3. Este paso está relacionado con la **información personal** que se comparte directamente en el perfil. Es muy importante considerar el fin específico de compartir datos como la dirección, el teléfono o el correo electrónico. Es básico tener en cuenta que a mayor información personal compartida, mayor será el riesgo de sufrir ataques a través de la Ingeniería Social.

De esta forma, se finaliza el proceso de comprobación rápida de la privacidad en los perfiles de Facebook. Siguiendo estos pasos, el usuario puede revisar los parámetros y niveles de privacidad, sin embargo, si se quiere realizar un análisis más profundo, éste debe realizarse desde el menú **"configuración".**

Twitter

1. Desde **“Perfil y Configuración”**, en la pestaña **“Seguridad y Privacidad”**, se pueden seleccionar las opciones: no permitir ser etiquetados en fotografías que suban a la red otros usuarios; dejar visibles los tuits solo para tus contactos; no desvelar la ubicación geográfica desde donde se tuiteó.
2. También se puede personalizar la opción de no permitir que el usuario sea localizado por su dirección de correo electrónico.

WhatsApp

1. Abrir el menú “**Ajustes**” y acceder a “**Cuenta**” para ver las opciones específicas de la esta.
2. De las cuatro opciones que podemos utilizar, seleccionamos “**Privacidad**” y vemos el menú que nos ofrece.
3. Podemos configurar acceso a nuestra información para aquellas personas que nosotros decidamos, así como, la hora de la última conexión, foto de perfil y estado.
4. Cada apartado nos ofrece tres opciones: dejarse abierto a todos, solo para contactos o bloqueado para todos.
5. Finalmente, también puede seleccionarse los contactos que pueden intercambiar mensajería con nosotros.

Instagram

1. Pasos para configurar una **cuenta** de Instagram como **privada**:
   - Acceder al perfil personal mediante el **icono en forma de persona.**
   - Pulsar el icono de “**Configuración de parámetros”.** Es un icono de una rueda dentada (iPhone) o tres puntos verticales (Android).

- En los **Ajustes de cuenta**, activar la pestaña "**Cuenta privada**", ésta pasará de color gris a azul.
- Aparecerá un *check* de confirmación; presionar **"Sí, estoy seguro"**, y la cuenta de Instagram será privada.

2. **Bloquear un usuario** en la aplicación:
   - Accedemos al **perfil del usuario** que deseamos bloquear. Se puede hacer con particulares, marcas u organizaciones.
   - Una vez en el perfil, pulsar el icono de "**Configuración de parámetros**". Es un icono en forma de rueda dentada (iPhone) o tres puntos verticales (Android).
   - Tenemos dos opciones: **bloquear** a ese usuario o **denunciar** al administrador que ese perfil transmite contenido inapropiado.
   - Un mensaje nos confirma que el usuario ha sido bloqueado en Instagram.
   - Así nadie podrá seguirnos sin nuestra aprobación, ni podrá ver las fotos que publicamos. Tampoco se podrá buscar nuestra cuenta, parecerá que se haya eliminado.
   - Sin embargo, si nuestra cuenta está configurada como pública, sí se podrá acceder mediante los comentarios que hayamos hecho en fotos de otros usuarios, o escribiendo la dirección en el navegador web.

Snapchat

1. Al iniciar sesión, activaremos la **sesión en dos pasos** para evitar que otras personas puedan atacar e iniciar sesión con nuestros datos y suplantar nuestra identidad:
   - Al abrir "**Ajustes**" se verá un menú desplegable donde elegimos **"Verificar inicio de sesión".**
   - Se puede seleccionar el tipo de verificación en dos formas: por SMS o mediante una aplicación.
   - También se puede "olvidar dispositivos" verificados previamente.

2. Después, volvemos al menú **"Ajustes"** y seleccionamos la opción **"Quién puede":**
   - En este apartado podemos especificar al programa quién va a poder contactar con nosotros o acceder a "Mi historia".
   - De esta forma ninguna persona no deseada pueda contactar con nosotros o acceder a los datos que compartimos.

Periscope

1. La aplicación Periscope conecta con los datos de las cuentas de Twitter, por lo que copiará el mismo perfil que tengas en esta aplicación.
2. Una vez dentro, hay **4 iconos** que representan las funciones de la aplicación:
   - **TV:** indica las últimas conexiones de las personas que sigues.
   - **Globo terráqueo:** indica qué conexiones se están produciendo en ese momento a nivel global.
   - **Cuadrado con punto rojo**: nos lleva a la pantalla para emitir en directo.
   - **Icono con tres personas**: nos dice qué contactos de Twitter tienen cuenta de Periscope.
3. Cuando vamos a **emitir en directo**, hay que tener en cuenta los siguientes ajustes:
   - Activa o desactivar el **modo localización**. Esta opción facilita poder saber desde dónde se está realizando la conexión.
   - Permite hacer un ***streaming*** **privado**, teniendo acceso a él únicamente aquellas personas que nosotros decidamos.
   - Activa o desactiva los **comentarios**, permitiendo que cualquiera interactúe con nosotros.
   - Activa o desactiva la opción del **tuit**, informando automáticamente en Twitter que estamos retransmitiendo.

Ask.fm

En esta aplicación existen una serie de opciones con respecto a la **recopilación**, **uso** y **divulgación** de la información personal a través de los servicios, incluida la posibilidad de evitar que otros usuarios nos envíen preguntas.

1. La pestaña "**Privacidad**" de la página de "**Configuración**" permite:
   - Desactivar las preguntas anónimas.
   - Ocultar nuestras respuestas para que no aparezcan en la sección "en directo".
2. La pestaña "**Notificaciones**" de la página de **"Configuración"** (en el móvil) permite la opción de no recibir notificaciones de Ask por email, como publicidad de productos y servicios de Ask.fm.
3. **Bloqueo de otros usuarios**. Se puede incluir a cualquier usuario en una "lista de usuarios bloqueados" haciendo clic en el botón **"Bloquear en el perfil"** de ese usuario. Esto evitará que esa persona nos haga preguntas.

YouTube

1. Configuración de **privacidad de los vídeos**. Para hacer que todos los vídeos que se suban en YouTube sean privados habrá que:
   - Acceder a la cuenta personal de YouTube.
   - Desplegar el menú **"Mis vídeos".**
   - Elegir el vídeo y hacer clic en **"Editar",** bajo la miniatura del vídeo.
   - Ir a las **"Opciones"** para compartir y emitir vídeos y buscar la sección "**Privacidad**", donde se pueden establecer los vídeos como:
     - **Público**: función predeterminada, da acceso para todo el mundo.
     - **Oculto**: es un tipo específico de vídeo privado, pudiendo verlo solo las personas a las que se les envíe el enlace.

- **Privado**: solo pueden verlo los usuarios elegidos. No aparecen en nuestro canal ni en las búsquedas.

2. Habilitar el **modo restringido** para ocultar vídeos que podrían incluir contenido poco apropiado: desplázate a la parte inferior de cualquier página de YouTube y haz clic en el menú desplegable de la sección **"Modo restringido".** Selecciona **"Sí"** para habilitar esta función en este navegador.

3. Recientemente, YouTube presentó su versión infantil: "**YouTube Kids**", https://kids.youtube.com/, que nos ofrece una serie de opciones para controlar el tipo de vídeos que nuestros hijos pueden visualizar.
   En esta versión no hace falta registrarse o iniciar sesión, para que no se quede grabado ningún dato personal del niño. Por esa razón, tampoco es posible subir vídeos, dar a "me gusta", ni compartir o comentar ningún vídeo que aparezca.
   El control parental de YouTube Kids incluye:
   a) **Temporizador**: para limitar el tiempo que los pequeños invierten en este nuevo canal. Nos saltará una alarma para avisarnos de que ya han visto suficiente.
   b) **Ajustes de sonido**: ofrece la posibilidad de silenciar y disminuir el volumen de la música y los efectivos de sonido.
   c) **Ajustes del buscador**: Podremos preseleccionar ciertos vídeos en la pantalla principal para que no haya necesidad de buscar otro contenido, pudiendo apagar la opción del buscador. Igualmente está habilitada la búsqueda por voz, para aquellos niños que no saben escribir.
   d) ***Feedback***: al ser una versión inicial, piden a los usuarios retroalimentación para poder mejorar la aplicación y adaptarla lo mejor posible a las necesidades que exigen los menores.

Legislación

Ley Orgánica 5/2000

- Responsabilidad penal de los **menores**:
    - Art. 7: Menores de 14 años inimputables. Aunque tengan condición de menores, este artículo establece consecuencias tales como internamiento en centros de menores, tratamiento ambulatorio, asistencia a centros de día, libertad vigilada, prestación de servicio a la comunidad, tareas socio-educativas, etc.

- Responsabilidad penal de los **padres**:
    - Art. 61.3: En el pago de las responsabilidades de menores de 18 años, los padres, tutores o guardas legales responderán solidariamente de los daños y perjuicios.

Código Civil

- Responsabilidad de los centros **educativos**:
    - Art. 1903: Personas o entidades titulares de un centro docente de enseñanza no superior, responderán por los daños y perjuicios que causen sus alumnos menores de edad durante el tiempo que estén bajo control y vigilancia del profesorado del centro.

Ley Orgánica 1/1996 de Protección Jurídica del Menor

- Artículo 5: Derecho a la información

1. *Los menores tienen derecho a buscar, recibir y utilizar la información adecuada a su desarrollo.*
Se prestará especial atención a la alfabetización digital y mediática, de forma adaptada a cada etapa evolutiva, que permita a los menores actuar en línea con seguridad y responsabilidad y, en particular, identificar situaciones de riesgo derivadas de la utilización de las nuevas tecnologías de la información y

la comunicación así como las herramientas y estrategias para afrontar dichos riesgos y protegerse de ellos.
2. Los padres o tutores y los poderes públicos velarán porque la información que reciban los menores sea veraz, plural y respetuosa con los principios constitucionales.

NOTA INTERNA PARA PADRES Y PROFESORES

Normas esenciales para los padres

- Ser un ejemplo a seguir: no se puede exigir al menor lo que uno mismo no cumple.
- Establecer normas y límites claros y razonables, a través del consenso familiar.
- Promover el equilibrio entre el uso de las TIC y el resto de actividades del menor.
- Preparar un entorno TIC ajustado a la madurez del menor.
- Conocer y usar las herramientas de control parental.
- Ayudarles a ser críticos con lo que encuentran en la red, para que aprendan a contrastar siempre la información a la que acceden.
- Enseñar a gestionar su privacidad y su imagen.
- Inculcar el respeto a los demás, enseñar netiqueta.
- Enseñar a crear contraseñas seguras y proteger los dispositivos.
- Trasmitir confianza para tratar cualquier tema, evitando la sobrerreacción y el juicio rápido.
- Conocer el entorno digital y la tecnología, intentar estar al tanto de lo que es popular entre menores.

Cómo reaccionar ante un incidente

La falta de una mediación parental eficaz puede facilitar incidentes relacionados con el uso inadecuado de las TIC como *ciberbullying*, *sexting*,

grooming, tecnoadicciones, suplantación de identidad, establecimiento de vínculos con comunidades peligrosas, infección por virus o fraudes, acceso a contenidos inapropiados, etc. El abordaje de estos casos, a pesar de sus diferencias, se basa en algunas pautas comunes:

1. Crear un clima de confianza para que el menor comunique el problema.
2. Escuchar, dialogar y recabar toda la información posible antes de llegar a alguna conclusión y empezar actuar.
3. Reforzar su autoestima y no culpabilizar, es importante que el menor se sienta apoyado tras haber cometido un error.
4. Esbozar un plan, acordarlo con el menor y hacerle partícipe en la solución del problema.
5. Comunicar al centro educativo, aunque no esté directamente vinculado con el incidente, la situación de nuestro hijo.
6. Informar al pediatra sobre lo ocurrido, ya que en ocasiones estas situaciones pueden perjudicar la salud física o psicológica de los menores.
7. Asesorar cómo actuar ante futuras situaciones de riesgo para que pueda aprender de su experiencia y estar más protegido en el futuro.
8. Buscar la ayuda de expertos cuando observemos que la situación sobrepasa nuestras capacidades para ayudar a nuestros hijos.
9. Notificar y denunciar las situaciones graves a la Policía Nacional, la Guardia Civil o la Fiscalía de Menores.