Programa de Jornadas Escolares

Promoción del uso seguro y responsable de Internet entre los menores

---

Mediación parental

Charla sensibilización familias

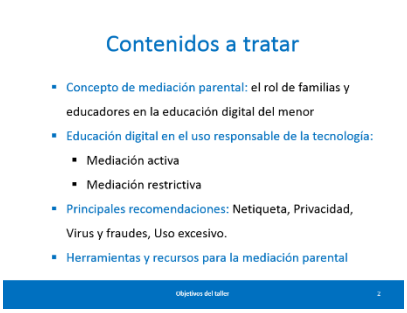
GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

Licencia de contenidos

CONTENIDO

TRANSPARENCIA 2: Contenidos a tratar



Si bien la protección y educación del menor en el ámbito de las TIC no se debe entender como exclusivamente de padres y madres, sí recae sobre ellos la principal responsabilidad, puesto que los menores en su relación con las TIC, precisan de la misma supervisión, acompañamiento y orientación, por parte de sus padres, que en cualquier otra actividad.

Por tanto, éstos deben conocer qué se entiende por Mediación Parental, en qué consisten las principales estrategias de mediación parental y finalmente conocer las principales recomendaciones en torno a las pautas de buen comportamiento en la red, cómo sensibilizar sobre la necesidad de una apropiada gestión de la privacidad, proteger los diferentes dispositivos de virus y fraudes y dominar las medidas de prevención ante el uso excesivo de las TIC.

- Entender el concepto de mediación parental: el rol de las familias y educadores en la educación digital del menor
- Educación digital en el uso responsable de la tecnología:
  - Mediación activa
  - Mediación restrictiva
- Principales recomendaciones:
  - Netiqueta
  - Privacidad, identidad digital y reputación online
  - Protección ante virus y fraudes y seguridad en dispositivos
  - Uso excesivo de las TIC
- Herramientas y recursos para la mediación parental

TRANSPARENCIA 3: Educación Digital de los menores

Hoy nadie niega las enormes oportunidades que las tecnologías nos ofrecen prácticamente en todos los aspectos de la vida. Y son precisamente los jóvenes quienes las han adoptado con mayor naturalidad.

Ellos rápidamente observan sus beneficios, la confianza en sus propias habilidades y la falta de prudencia propia de estas edades, les hace avanzar en su adopción, especialmente ante nuevos servicios y aplicaciones, pero también esta excesiva confianza les proporciona una falsa sensación de seguridad, y les hace considerar los riesgos vinculados al uso de la tecnología, como fácilmente evitables.

Por otra parte, debemos añadir que el contacto con la TIC por parte de los menores cada vez se produce a edades más tempranas. Por ello, la educación en el uso de las tecnologías debe ser algo prioritario en la etapa en la que nos ha tocado vivir.

TRANSPARENCIA 4: Mediación parental: definición

Se hace imprescindible, por tanto, un acompañamiento del menor por parte de los responsables de su educación.

Así, debemos entender el concepto de **Mediación Parental** referido a las TIC como*: "el proceso por el cual los responsables de la educación digital del menor, acompañan a éste en su proceso de alfabetización digital, le educan para que realice un uso responsable y seguro de las nuevas tecnologías y velan para impedir que los riesgos de las TIC se materialicen y en caso de ocurrir, ofrecer soluciones*". Definición extraída del **Monográfico sobre Mediación parental de RED.es**

Acompañar	Educar en el uso seguro y responsable	Velar. Reducir riesgos	Ofrecer soluciones

Evidentemente a nadie se les escapa que muchos padres y madres se sienten desbordados por el rápido avance del entorno digital, sintiéndose inseguros a la hora de abordar la prevención y mucho más cuando se trata de adoptar medidas, ante una situación de riesgo.

En este sentido los padres deben saber que esta responsabilidad no recae exclusivamente sobre ellos. En este proceso educativo, deben estar necesariamente implicados todos los agentes que tienen algo que aportar en la educación del menor: padres/madres, tutores, educadores y otros profesionales.

En estos momentos, se está avanzando mucho para que las competencias relacionadas con la seguridad y la responsabilidad de las TIC se incluyan en el currículum escolar. Tanto desde el gobierno, como desde la sociedad civil, se impulsan iniciativas que ayuden a las familias a identificar, tanto los aspectos positivos de las TIC para los menores, como los riesgos.

TRANSPARENCIA 5: Mediación Parental. Ejemplos

La web de la OSI (**https://www.osi.es**) y la sección de Escuela Cibersegura de Internet Segura for Kids (**https://www.is4k.es**) son un ejemplo de estas iniciativas. También la Policía se implica en sensibilizar y formar a los menores para minimizar los riesgos inherentes al uso cotidiano de las TIC.

Se propone, a continuación, a modo de introducción de los aspectos que vamos a tratar, visualizar el vídeo '**Las diez reglas de la Policía para el uso seguro de Internet entre menores'**: (Duración 1'19'')

La Policía Nacional ha elaborado un decálogo con una lista de **diez puntos que los padres tienen que comprobar del uso tecnológico de sus hijos.** Entre estos consejos se encuentra:

- revisar qué fotos han hecho, guardan y comparten en los dispositivos,
- velar por la intimidad de los menores y de quienes también aparecen en las fotos que han publicado,
- tener una correcta configuración de sus perfiles sociales, cerrados a su círculo personal, evitando introducir en ellas a personas desconocidas,
- protegerse frente a situaciones de acoso/ ciberacoso,
- evitar ser autores de delitos, como en el que incurrimos cuando compartimos imágenes y/o vídeos íntimos, de terceras personas.

TRANSPARENCIA 6: Educación digital

La educación digital debe vehicularse a través de una doble vertiente:

- **Educación tecnológica**: enseñando a los menores a utilizar las tecnologías con las garantías adecuadas de seguridad, privacidad y prevención.
- **Educación conductual**: por ejemplo, mostrando a los menores el respeto a la privacidad, la imagen, la netiqueta o buenos modales en la Red, etc.

TRANSPARENCIA 7: Regla básica en la Mediación Parental

Existe una regla básica de prevención en el uso seguro de las TIC normalmente conocida como la "regla de las tres R":

- R de **regular**: regular el acceso, el tiempo de conexión, los contactos.
- R de **reducir**: reducir los riesgos de las TIC con las recomendaciones generales de prevención.
- R de **recursos**: dotar al menor de recursos, para que sea él mismo el que vele por su propia seguridad.

A continuación, se facilitará información sobre cómo abordar cada uno de estos aspectos.

TRANSPARENCIA 8: Estrategias de Mediación activa

Para fomentar un uso positivo y seguro de Internet una de las estrategias más efectivas es la mediación activa, que implica supervisar, acompañar y orientar al menor en su relación con las TIC.

Supervisarle presencialmente, al menos en los comienzos, acompañándole en la exploración y en el aprendizaje. Por ejemplo, dialoga sobre qué utilidades tiene la red, cómo y para qué se usa, y la importancia de comportarse en la red de forma segura y responsable al igual que fuera de ella.

Compartir una actividad refuerza la confianza ayudando a que vuestros hijos os trasladen sus reflexiones, sus dudas y preocupaciones.

Presta atención a lo que hace mientras está conectado	Supervisa, acompáñale durante la búsqueda y su aprendizaje	Dialoga sobre el uso de Internet y el comportamiento seguro y responsable	Crea un clima de confianza y respeto mutuo

TRANSPARENCIA 9: Algunas pautas para realizar una Mediación activa

- **No demonices las tecnologías**. Ya es básica en casi todos los aspectos de la vida y será fundamental para el desarrollo tanto personal, como profesional de tu hijo.
- **Fórmate**. No hace falta ser un experto, pero si tu hijo percibe tu desconocimiento del medio, difícilmente querrá que le acompañes en la exploración de Internet, además de no tomar en serio tus recomendaciones.

- **Elige contenidos apropiados para su edad**. Ayúdale a descubrir sitios que promuevan el aprendizaje, la creatividad y que profundicen en sus intereses. Algunos contenidos de Internet pueden ser perjudiciales para su educación y desarrollo. Apóyate en herramientas de control parental, de las que hablaremos más adelante, para monitorizar y controlar los contenidos a los que accede tu hijo, a edades tempranas pueden resultar de mucha utilidad.
- **Interésate por lo que hace conectado**. Al igual que te interesas por sus amistades del colegio, del barrio… debes hacerlo por las amistades de tu hijo en la red, o las aplicaciones y juegos que más le interesan. Compartir actividades, por ejemplo, configurando las opciones de privacidad de las redes sociales, echándole una partida a un juego online, viendo vídeos o visitando páginas de interés común, es una buena forma de supervisar su actividad en Internet y trasladarle nuevos puntos de vista con la intención de sensibilizarle.
- **Sé el mejor ejemplo para tus hijos**. Antes de poner normas, piensa que estás obligado a cumplirlas, se coherente y haz exactamente lo que le pides a tu hijo. Dicen que educar con el ejemplo no es una manera de educar, es la única.

- **Evita el juicio rápido y asegúrate que se siente cómodo solicitando tu ayuda**. Si tu hijo presiente que se meterá en problemas al trasladarte, por ejemplo, algún comportamiento inadecuado, será más reticente a solicitar tu ayuda. Lo que puede provocar que intente resolverlo por sí mismo, tal vez, acrecentando el problema.

TRANSPARENCIA 10: Mediación activa (II)

Enséñale a:

- **Pensar críticamente.** Es necesario entender que no todo lo que ve en Internet es cierto. Ensénale a desconfiar de las apariencias y a contrastar la información en caso de duda.
- **Mantener la información personal en privado**. Explícale la importancia de no compartir determinadas imágenes e información personal y familiar como domicilio, nombres, teléfonos, costumbres, horarios, colegios… de gestionar adecuadamente las redes sociales y servicios que use en Internet, de cerrar sesiones y cuentas cuando no esté utilizando su dispositivo, y las consecuencias posibles de compartir dicha información.
- **Respetar a los demás**, igual en la calle que en Internet por lo que, por ejemplo, no debe subir imágenes de terceros sin su permiso.
- **No fiarse al 100% de con quién habla en Internet**. En el mundo digital es fácil hacerse pasar por otro, por ejemplo, a través del robo y suplantación de la identidad digital.
- **Crear contraseñas seguras y robustas y a proteger sus dispositivos**, para evitar pérdidas de información o virus informáticos con los que luego controlen nuestros dispositivos para poder cometer fraudes y delitos en nuestro nombre.
- Muéstrale la importancia de tener **los dispositivos que no se esté utilizando desconectados de Internet y apagados**, así como, desconectadas todas sus opciones de conectividad si no se utilizan (wifi, GPS, Bluetooth, etc.).
- Usar programas originales, a actualizar los programas, antivirus y sistemas operativos, y **reducir el riesgo de infecciones** no clicando en adjuntos de desconocidos o enlaces de dudosa procedencia.
- **Mantener un equilibrio en el tiempo de uso de las TIC**, para no perderse otras opciones, por ejemplo, de ocio al aire libre.

TRANSPARENCIA 11: Otro tipo de mediación es la restrictiva

La mediación restrictiva consiste en establecer normas y límites bien definidos, y exigir que se respeten. Pueden ayudar al menor a evitar riesgos y a promover un comportamiento responsable en el uso de la red.

En este caso, siempre atendiendo al sentido común y a la madurez del menor. Fáciles de cumplir, y que se conviertan en rutinas desde el primer momento.

Ejemplos:

- Edades de acceso a Internet y al primer móvil.
- Cuándo y por cuánto tiempo pueden estar conectados.
- Qué tipo de aplicaciones y servicios pueden usar: correo electrónico, mensajería instantánea, apps de juegos, etc.
- Restringir el uso del teléfono móvil durante las horas de sueño y comidas.
- Etc.

Establecer pactos familiares y escritos que recojan este tipo de normas suele ser un buen método. Lo situaremos en un espacio fácilmente visible para los pequeños con objeto de ayudarles a recordar los compromisos adquiridos. En la siguiente diapositiva veremos ejemplos de pactos familiares.

Cuando estamos hablando de edades tempranas, apoyarse en las herramientas de control parental, programas disponibles para todo tipo de dispositivos (ordenadores, tabletas, móviles y consolas) que permiten a los padres controlar ciertos aspectos de la vida digital de sus hijos, puede ser una opción.

Estos programas facilitan, entre otros aspectos:

- Bloqueo de páginas por palabras clave.
- Control del tiempo de uso del dispositivo
- Bloqueo de programas y aplicaciones.
- Crear listas blancas y negras: páginas a la que se permite acceder y páginas que estarán bloqueadas.
- Monitorización del historial de búsquedas realizadas con el navegador.
- Herramientas que bloquean la información que sale del ordenador

Hay que tener en cuenta que esta opción, hacer uso de herramientas de control parental, siempre debe ir acompañada de nuestra orientación, asesoramiento, etc. No son soluciones 100% efectivas, pero a edades tempranas pueden resultar útiles como complemento a la educación digital del menor.

Preparar un entorno TIC ajustado a la madurez del menor es otra medida que nos ayudará a evitar sorpresas. Conviene preparar los entornos de trabajo del menor para que sean adecuados a su madurez, eliminando la posibilidad de exponerle a riesgos innecesarios. Por ejemplo, utilizando cuentas de usuario específicas o facilitándole buscadores y navegadores infantiles.

Vamos a ver en mayor detalle estos 3 aspectos a continuación.

TRANSPARENCIA 12: Ejemplos de pacto familiar

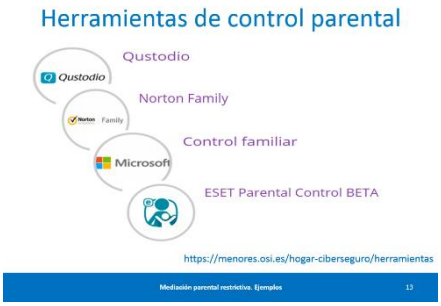
En la red podéis encontrar diferentes ejemplos de pacto o acuerdo familiar.

El Grupo de Redes Sociales de la Policía Nacional ha elaborado un “acuerdo” para que padres de hijos menores de 13 años fijen con ellos por escrito, unas normas de buen uso de su móvil, tableta, ordenador o dispositivo conectado a Internet, a pactar entre todos cuando se vaya a comprar o estrenar un nuevo gadget para el chico/a.

Otro ejemplo nos lo proporciona una madre americana con 18 reglas que pidió a su hijo para tener y usar un móvil. Interesante la última regla: **Meterás la pata.** *"Te quitaré el teléfono. Nos sentaremos y hablaremos sobre ello. Volveremos a empezar. Tú y yo siempre estamos aprendiendo. Somos un equipo. Estamos juntos en esto."*

Nosotros os proponemos el elaborado por IS4K **Contrato familiar para el buen uso de una Tablet.**

TRANSPARENCIA 13: Herramientas de control parental



Los padres deben conocer la existencia de herramientas de control parental y decidir su utilización o no, siendo conscientes que cualquier herramienta de control parental por sí sola no sirve, debe ir siempre acompañada de orientación, apoyo, asesoramiento.

Se llama control parental a cualquier herramienta o programa tecnológico que permita a los padres controlar y/o limitar el uso que un menor pueda hacer del dispositivo o de Internet. Hoy en día tenemos una grandísima oferta de programas de control parental, tanto de forma gratuita como de pago, pero también podemos encontrar opciones de control parental en muchos dispositivos y programas que ya veníamos utilizando.

Podemos encontrar herramientas de este tipo en:

- Los principales sistemas operativos que utilizamos (Windows, MacOS, Android, Linux, iOS…)
- Plugins o programas que se anexionan a nuestros principales navegadores (Internet Explorer, Google Chrome, Mozilla Firefox…) permitiendo opciones de control parental para la navegación.
- Herramientas web y software específico, de pago o gratuitos, que descargamos en nuestros dispositivos (ordenadores, tabletas y móviles) y nos ofrecen multitud de opciones. En la siguiente página: **https://www.is4k.es/de-utilidad/herramientas** se detallan varias herramientas gratuitas de control parental.
- Routers, que proporcionan el acceso a Internet, que ofrecen opciones de control parental.
- Opciones de control parental que brindan los principales Proveedores de Servicios (ISP), aquellas compañías que nos ofrecen la conexión a Internet en nuestros dispositivos y que también brindan opciones y programas de control parental a los usuarios.
- En las actuales videoconsolas, así como en las modernas Smart Tv o la TDT, ofrecen opciones de control parental que deben ser exploradas y configuradas.

Acceder si tenemos conexión: **https://www.is4k.es/de-utilidad/herramientas** dónde se detallan varias herramientas gratuitas.

TRANSPARENCIA 14: Cuentas de usuario específicas

A través de una configuración adecuada podremos mitigar los riesgos específicos a los que están expuestos los menores, tal y como veremos a continuación.

Seguridad de nuestra información y archivos.

Si cada miembro de la familia que utiliza el equipo lo hace con su cuenta y usuario particular, se reduce el riesgo de pérdida de información debido a fallos y errores no intencionados. Esto es debido a que asociado a cada cuenta de usuario, existe un entorno aislado que sólo es accesible por el usuario en cuestión. Gracias a esto, evitaremos que, por ejemplo, alguien borre nuestros documentos de trabajo al intentar desinstalar una aplicación, mayor protección frente a virus, troyanos, etc. Si nuestro equipo se infecta mientras estamos usando una cuenta de usuario estándar, el impacto será menor ya que al tener menos permisos y acceso a menos recursos, el virus está más contenido y su eliminación será menos costosa. Por lo tanto, la cuenta de Administrador sólo la utilizaremos cuando sea estrictamente necesario.

Protección infantil

Configuraremos cuentas específicas para los más pequeños, con las medidas de seguridad necesarias para ellos. Son muchos los aspectos que se pueden controlar en relación a las cuentas para menores pero lo más habitual es considerar las siguientes funcionalidades:

- Permite boquear o autorizar el uso específico de aplicaciones que ya estén instaladas en el equipo.
- Permite acotar el tiempo que el menor está conectado.
- Permite bloquear o autorizar el acceso a páginas web.
- Permite obtener informes sobre la navegación.

De todas formas, no debemos olvidar que aunque la cuenta de usuario que utilice el menor esté restringida, es recomendable supervisar su actividad y seguir orientándole para que haga un uso seguro y responsable de la tecnología como hemos venido comentando a lo largo del documento.

Acentuaremos la importancia de que lo ideal sería encontrar un equilibrio entre la Mediación activa y la restrictiva, combinándolas en función de la madurez del menor y de los requisitos de privacidad que demande, ambos aspectos relacionados en gran medida con su edad.

TRANSPARENCIA 15: Recomendaciones específicas adecuadas a cada grupo de edad

A medida que los menores crecen, cada vez será más difícil mediar en su actividad en Internet. El adolescente busca su propia identidad y demandará unos requisitos de privacidad mayores.

Según vamos apreciando signos de madurez en su comportamiento iremos ajustando el nivel de mediación, para que vaya aprendiendo a gestionar las situaciones por sí mismo.

En esta transparencia se ofrece un marco orientativo de pautas sobre las que podéis trabajar en función de la edad de vuestro hijo.

- **NIÑOS PEQUEÑOS 3 a 5 años.** Primer contacto con las tecnologías. Se recomienda una supervisión total de sus actividades, e iniciarles en las pautas básicas de uso.
- **NIÑOS 6 a 9 años.** Sus primeros pasos en Internet. Continuar con una estrecha supervisión, mientras se van ampliando los usos y las buenas prácticas asociadas.
- **JÓVENES ADOLESCENTES 10 a 13 años.** Uso intensivo de Internet: redes sociales, juegos en línea y móviles. Deben comenzar a desarrollar habilidades para tomar decisiones de forma independiente. Seguir muy de cerca sus evoluciones
- **ADOLESCENTES + 14 años.** Resulta más difícil mediar en sus actividades en línea. Empezar a confiar en lo que se les ha enseñado, pero asegurándose de que se preocupan por mantenerse a salvo.

TRANSPARENCIA 16: Netiqueta: Comportamiento en línea

Desde el principio es conveniente hablar de la Netiqueta: pautas de buen comportamiento para comunicarse en la red y fomentar que ésta sea cada vez más agradable y segura para todos.

Enséñale que la red, al igual que toda comunidad tiene sus normas y debemos conocerlas para movernos con educación y seguridad.

- Por ejemplo, escribir en mayúsculas en Internet significa 'gritar', por lo que no es adecuado utilizarlas.
- **Pensar antes de escribir opiniones, comentarios**, etc. Igual que en la vida real, existen muchas formas de expresar nuestra opinión e incluso defenderla, sin faltar ni molestar a nadie. Recuérdales que al otro lado de la línea también hay personas.
- **Respetar la privacidad de los demás.** No hay que facilitar ni publicar nunca datos personales de terceros sin su previo consentimiento.
- **Pedir las cosas con educación.** No somos el centro de atención del ciberespacio. Hay que aprender a ser pacientes y a pedir las cosas con respeto y educación. La inmediatez es una de las ventajas y desventajas de Internet.
- **Respetar los horarios de todos**, igual que no llamamos a un amigo a las 2 de la madrugada entre semana, tampoco es apropiado mandarle un WhatsApp.
- No todos los servicios tienen las mismas reglas de buen uso. Es recomendable **observar** cuando se esté en una nueva red o utilizando un nuevo servicio **y aprender**.

TRANSPARENCIA 17: Netiqueta. Comportamiento en línea (II)

Edúcale en la sensibilidad y el respeto, desde bien pequeños. Trasládele la regla de oro: "aquello que no nos gustaría que nos hicieran a nosotros, no deberíamos hacérselo a los demás".

Que sea consciente de que en Internet no todo vale y que hay 'bromas' que pueden acabar mal, llegando incluso a actuar la ley.

Por este motivo, una buena práctica de Netiqueta es precisamente la **necesidad de empatizar**, la habilidad de entender y compartir las emociones y las experiencias de los otros, aunque no los tengamos cara a cara.

TRANSPARENCIA 18: Comunicación familiar

La **comunicación familiar** contribuye a que se establezcan y se estrechen unos vínculos que facilitarán que los hijos recurran a los padres en caso de necesidad o problemas. De este modo, uno de los pilares clave de la prevención es **transmitir a los hijos una información clara y objetiva** respecto a los riesgos y cuáles son las consecuencias del uso inapropiado de las tecnologías.

Es imprescindible que el padre o la madre tengan o adquiera conceptos mínimos sobre las TIC, ya que es fundamental que se establezca un vínculo de confianza con el menor en torno a las TIC

Antes de ofrecer nuestra perspectiva y darles la información oportuna, debemos informarnos sobre lo conocen, qué quieren y deben saber y su percepción personal sobre los riesgos de las tecnologías. En este sentido, la información que debemos transmitirles debe ser:

- Desmontar opiniones e ideas equivocadas sobre el uso de las TIC.
- Informar a los hijos sobre los riesgos físicos y psicológicos del uso excesivo e irresponsable.
- Ayudarles a comprender los riesgos de una conducta inadecuada en la Red: imposibilidad de borrar de la Red lo compartido y colgado, las posibles denuncias y consecuencias legales, las consecuencias para los afectados y su entorno, el detrimento de la propia imagen al obrar de mala fe, consecuencias en el futuro personal y laboral, etc.

El hecho de que a los menores se les considere nativos digitales no quiere decir que sean competentes digitales. La competencia digital se refiere a las capacidades y habilidades para interactuar con las herramientas tecnológicas, con la finalidad de sacarles el máximo provecho y hacerlo de una forma segura

TRANSPARENCIA 19: Los peligros del acoso en Internet

Por ejemplo, **sensibilízale sobre un riesgo que desgraciadamente se está incrementando y que puede llegar a ser muy grave: los riesgos del acoso a través de Internet**: *ciberbullying* (actitud de acoso a través de las nuevas tecnologías, llevada a cabo entre iguales y con intención de dañar a la víctima, de forma consciente y reiterada) y el *grooming* (de estrategias que un adulto emplea para acercarse a un menor con intenciones de carácter sexual), y **edúcale en la sensibilidad y el respeto**.

Aconsejándole a **mantener la información sensible en privado**. Recuérdale que no se tiene control sobre lo que se pública a través de Internet y que alguien podría utilizarlo en el futuro para perjudicarle.

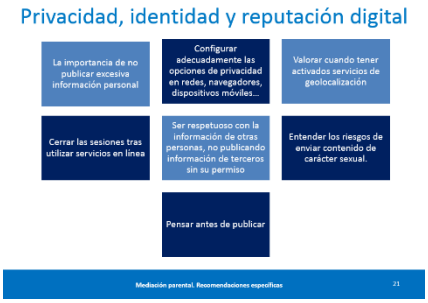
- Enséñale a **no responder a las provocaciones y a los malos modos** de otros.
- **Fomenta la empatía**. Ayuda a tu hijo a comprender el impacto perjudicial del ciberacoso sobre las víctimas, en el presente y en el futuro. Incentívalo a escuchar a las víctimas y a prestarles apoyo. Anímale a mostrar su rechazo.
- **Denunciar los abusos**. La mayoría de servicios en la red (redes sociales, mensajería instantánea, etc.) permiten denunciar contenidos (fotografías, comentarios e incluso perfiles) que resulten ofensivos. Fomenta el uso de los mecanismos de denuncia para animarle a construir una red más respetuosa. **Anímale a romper la cadena**. A que si le envían comentarios o imágenes humillantes sobre otra persona debe ponerle freno y responder a esas personas diciendo que no le parece bien lo que están haciendo, que no quiere fomentarlo. Que anime a otras personas a hacer lo mismo.

TRANSPARENCIA 20: Privacidad, identidad digital y reputación

Debemos sensibilizar sobre la necesidad de una apropiada gestión de la privacidad, que facilite la creación de una identidad y reputación de provecho para el desarrollo personal y profesional del menor. Su identidad digital será su principal carta de presentación en el futuro.

Conciénciales de la **importancia de una búsqueda de equilibrio entre las virtudes de mostrarse públicamente y los riesgos que conlleva**.

TRANSPARENCIA 21: Recomendaciones específicas



- Muéstrales la relación entre la **sobreexposición de información personal** (teléfono, correo, horarios, lugar de residencia, geoposicionamiento, etc.) y sus riesgos asociados (spam, suplantación de identidad, fraudes, acoso, etc.).
- Sensibilízale sobre la importancia de **pensar antes de publicar.** En Internet no es posible controlar quién acabara viendo nuestros mensajes (la audiencia) ni eliminar los contenidos una vez publicados, lo que puede tener serias consecuencias, para su reputación (ej. búsqueda de trabajo).
- Hazle entender los **riesgos de enviar contenido de carácter sexual en las relaciones de pareja (sexting).** No es difícil que acaben haciéndose públicos (robo o pérdida del móvil, venganza por despecho...) y afecten a su reputación y a su autoestima. De igual modo, debe entender la problemática de difundir contenidos sensibles de terceros sin su consentimiento.
- Asegúrate de que conoce los mecanismos para gestionar la privacidad en aplicaciones y servicios web (navegadores, redes sociales, dispositivos móviles, etc.). Incúlcale conductas responsables, cómo no publicar o reenviar información de otras personas sin su permiso, no etiquetarles en fotos sin su consentimiento. Del mismo modo, se recomienda demandar esas conductas responsables en los demás (amigos, familiares o conocidos).
- Existen **virus que permiten grabar video a través de las cámaras de los dispositivos infectados**. Por este motivo, se debe evitar que las cámaras apunten directamente al espacio donde está el menor. Una buena opción es poner una pegatina que tape la cámara cuando no se esté utilizando.
- Recuérdale la necesidad de **cerrar las sesiones tras utilizar servicios en línea** (correo, red social), especialmente en aquellos ordenadores o dispositivos que son de otras personas, de cibercafés, de amigos, en wifi públicas.

TRANSPARENCIA 22: Protección ante virus y fraudes, y seguridad en dispositivos

Los delincuentes en Internet intentan engañarnos de numerosas formas con el objetivo de infectar los dispositivos con virus, caer en sus fraudes y acceder a nuestra información privada.

Aunque seamos nosotros quienes nos ocupemos de instalar antivirus y mantenerlos actualizados es conveniente que enseñemos a los menores. Pronto ellos tendrán que ser responsables de sus propios equipos

Prepara el sistema contra los virus:

- Instala un antivirus y mantenlo actualizado. Puedes encontrar soluciones antivirus gratuitas en la sección de **herramientas gratuitas** de la Oficina de Seguridad del Internauta (OSI).
- Mantén el sistema operativo (SO), el navegador y todas las aplicaciones actualizadas.

Protégete mientras navegas

También es necesario enseñarle a protegerse mientras navega. Los delincuentes utilizan técnicas de **ingeniería social** como reclamo para conseguir que actuemos de la forma que ellos desean. Por ejemplo, seguir un enlace a una página maliciosa, descargar y ejecutar un fichero manipulado, etc. Para captar la atención se apoyan en elementos que despierten nuestra curiosidad y morbo, por ejemplo, videos con personajes famosos, súper ofertas y premios, noticias de catástrofes, entre otros muchos.

TRANSPARENCIA 23: Recomendaciones específicas

Las principales recomendaciones a trasladar a los menores son:

- No hacer clic en enlaces que resulten sospechosos.
- No abrir ficheros adjuntos sospechosos.
- Desconfiar de los correos o mensajes de remitentes desconocidos.
- Solo descargar programas y apps desde sus páginas oficiales.
- Cuidar sus contraseñas. Muéstrale como generar contraseñas fuertes y aconséjale que no las comparta con nadie (tan solo con sus padres).

TRANSPARENCIA 24: Uso excesivo de las TIC

Es necesario que entendamos que en la sociedad actual, la conexión comienza a ser casi permanente. Y no por ello tenemos que estar hablando de adicción.

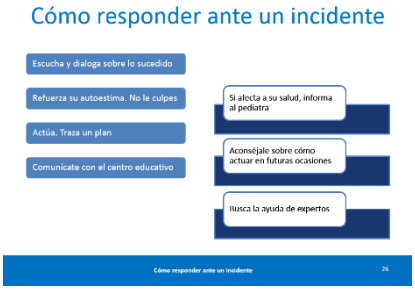
Aclararemos que un uso excesivo de las TIC, es aquella que limita la libertad de la persona por la gran dependencia que provoca, interfiriendo en la vida diaria de quien la padece y de sus allegados.

TRANSPARENCIA 25: Recomendaciones específicas

Para trabajar medidas de prevención ante un uso excesivo de las TIC, abordaremos con nuestro hijo recomendaciones como las siguientes:

- La importancia de **marcarse un horario de uso** cuando utiliza Internet como herramienta de ocio, tiempo libre y entretenimiento al igual que lo hace para cualquier otra actividad.
- La necesidad de **respetar los horarios** de dormir, comer y obligaciones domésticas.
- Además de utilizar Internet **buscar otras actividades alternativas** para su tiempo libre.
- **Cuidar las relaciones sociales** a través de la Red, pero hazlo también en persona.
- Será necesario **ofrecer apoyo y comprensión**. No convertirle en culpable, dares cuenta de que es víctima de una situación que no le resultará fácil reconocer ni abordar.
- **Buscar la ayuda de un especialista** en este tipo de conductas.

TRANSPARENCIA 26: Cómo responder ante un incidente



- **Escucha y dialoga.** Pregunta a tu hijo qué está sucediendo, escúchale atentamente y ayúdale a expresar emociones y preocupaciones. Para facilitar el diálogo muéstrate sereno y adopta una actitud de comprensión y atención, no es el momento de juzgarle. Si encuentras reticencias al diálogo, ten en cuenta que los adolescentes tienen su propia dinámica social que generalmente no incluye a sus padres. En ese caso, promueve que hable con amigos u otros adultos de confianza para que le ayuden a gestionar la situación.
- **Refuerza su autoestima y no le culpabilices**. Haz hincapié en que no está solo, que estás allí para ayudarle a resolver el problema, aunque haya cometido errores. Sé positivo, reconoce su valentía por haber pedido ayuda y/o dejarse ayudar y hazle saber que se solucionará.
- **Actúa, traza un plan.** Actúa inmediatamente, no esperes a que el incidente cese por sí solo porque el problema podría agravarse. Asegúrate de que el menor entiende cuáles son los siguientes pasos a realizar. El objetivo es que salga reforzado y se sienta parte de la solución.
- **Comunica la situación al centro educativo**. En caso de que el incidente esté vinculado con el centro educativo es muy importante que sean conocedores de la situación. Muchos de los centros educativos disponen de protocolos de actuación en sus planes de convivencia para gestionar estas situaciones (ej. ciberacoso escolar). Lo más importante es trabajar conjuntamente para resolver la situación.
- **Informa de lo ocurrido al pediatra**. En caso de que el incidente haya afectado a la salud del menor este debe ser valorado por su pediatra para tratar los síntomas que tiene, para prevenir que la situación empeore y para ayudarle en los pasos a seguir.

- **Aconséjale sobre cómo actuar ante futuras situaciones**. Se trata de evitar que el problema se reproduzca en el futuro. Trasládale las recomendaciones oportunas para minimizar las probabilidades de que vuelva a ocurrir. Ayúdale a aprender de sus errores sin culpabilizarle, haciéndole saber que todos nos equivocamos y que lo valiente es aprender de los errores.
- **Busca la ayuda de expertos**. Al final de la presentación se encontrará una página de Líneas de ayuda y sitios de denuncia ante un incidente.

TRANSPARENCIA 27 y 28: Recursos para la educación digital

Se recogen algunos recursos que puedan ayudar a las familias para ampliar información sobre Mediación parental, herramientas de control parental y de protección de dispositivos, así como líneas de ayuda y denuncia ante incidentes.

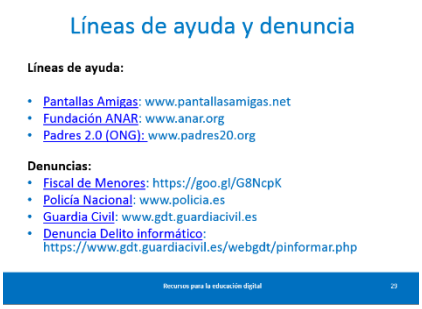
Recursos para la educación digital

- Guía para el uso seguro y responsable de Internet por los menores. Itinerario de Mediación Parental. Internet Segura for Kids
- Monográfico sobre Mediación Parental. Red.es
- Contrato familiar para el buen uso de una Tablet**.** Internet Segura for Kids
- Acuerdo buen uso móvil e Internet.pdf Policía Nacional
- Artículo "Orden en casa, Cada miembro de la familia con su cuenta de usuario. Oficina de Seguridad del Internauta
- Contrato que una madre exigió a su hijo para tener iPhone
- Herramientas de control parental Internet Segura for Kids
- Herramientas para la protección de tus dispositivos Oficina de Seguridad del Internauta.
- Formulario de alta de incidentes Oficina de Seguridad del Internauta.

Canal de ayuda de OSI

- Formulario de alta de incidentes
- Teléfono de atención: 901 111 121

TRANSPARENCIA 29: Líneas de ayuda y denuncia



Líneas de ayuda

- Pantallas Amigas: www.pantallasamigas.net
- Fundación ANAR: www.anar.org
- Padres 2.0 (ONG): www.padres20.org

Denuncia

- Fiscal de Menores: https://goo.gl/G8NcpK
- Policía Nacional: www.policia.es
- Guardia Civil: www.gdt.guardiacivil.es

- Denuncia Delito informático: https://www.gdt.guardiacivil.es/webgdt/pinformar.php

- Denuncia Delito informático: https://www.gdt.guardiacivil.es/webgdt/pinformar.php

TRANSPARENCIA 30: Donde localizar más información

Recomendaremos dos páginas imprescindibles para saber más y estar perfectamente actualizado:

La página de OSI Oficina de Seguridad del Internauta **https://www.osi.es** Destacar las siguientes secciones con información de interés:

- **Ponte al día (sección de actualidad):**
  - Avisos de seguridad
  - Blog
  - Historias reales
- **¿Qué deberías saber?**
  - Sobre tus dispositivos
  - Sobre tu información
  - Sobre el fraude
  - Sobre tus conexiones
  - Sobre tu actividad online

Y la página Internet Segura for Kids **http://www.is4k.es** con:

- La información que "**necesitas saber**" sobre privacidad, ciberacoso escolar, sexting, contenido inapropiado, uso y configuración segura, mediación parental.
- Artículos de interés y actualidad en el "**blog**".
- Guías, juegos, herramientas de control parental y otros recursos "**de utilidad**".
- Información de "**programas**" de sensibilización para un uso seguro y responsable de Internet por los menores.
- Una "**línea de ayuda**" con una serie de preguntas frecuentes y un contacto para resolver dudas.

TRANSPARENCIA 31: Despedida

Siempre podéis poneros en contacto con nosotros a través de la web:

- https://www.is4k.es

Internet Segura for Kids (IS4K), es el nuevo Centro de Seguridad en Internet para menores en España. Allí podéis encontrar información, guías, juegos y otros recursos de utilidad sobre los principales riesgos de Internet, cómo prevenirlos y afrontarlos. Además disponéis de una línea de ayuda con una serie de preguntas frecuentes y un contacto para resolver vuestras dudas.

Recordad que podéis seguir nuestros perfiles públicos de redes sociales:

- Facebook, buscando "Internet Segura for Kids"
- Twitter, usuario @is4k