Guía para familias

Manual del sentido común en Internet







Contenido

INTRODUCCIÓN A LA GUÍA	1
Objetivos de la Guía	1
¿CUÁNDO EMPEZAR A OCUPARNOS?	2
¿TENEMOS LA FÓRMULA MÁGICA?	3
FOMENTO DE VALORES	4
RESPETO	4
RESPONSABILIDAD	5
¿CUÁLES SON LOS RIESGOS?	6
Uso abusivo	6
ACCESO A CONTENIDOS INAPROPIADOS	6
VULNERACIÓN DE LOS DERECHOS DE PROPIEDAD INTELECTUAL	7
ACOSO SEXUAL O 'GROOMING'	7
AMENAZAS A LA PRIVACIDAD. POR EJEMPLO 'SEXTING'	7
DELITOS ECONÓMICOS Y FRAUDES	8
RIESGOS TÉCNICOS	8
CIBERBULLYING	9
Y AHORA ¿QUÉ HACEMOS?	10
RECOMENDACIONES GENERALES CUANDO TENGO UNA CONEXIÓN A INTERNET	10
RECOMENDACIONES SOBRE CONTENIDOS	14
RECOMENDACIONES SOBRE LOS REGISTROS EN LOS SERVICIOS DE INTERNET	15
RECOMENDACIONES SOBRE LOS SERVICIOS QUE UTILIZAMOS	17
RECOMENDACIONES SOBRE TELÉFONOS INTELIGENTES (SMARTPHONES)	21
RECOMENDACIONES SOBRE VIDEOJUEGOS	24
RECOMENDACIONES PARA EVITAR TENER PROBLEMAS CON LA LEY	25
CONCLUSIONES	27
GENERAR CLIMA DE CONFIANZA Y FOMENTO DE VALORES	27
ANEXO	28
IMÁGENES DE LA G UÍA	28
FUENTES Y BIBLIOGRAFÍA	28

INTRODUCCIÓN A LA GUÍA

Desde la sección de Participación Educativa, Atención al Profesorado y Convivencia de Gobierno de Navarra se os quiere hacer llegar esta guía para que sirva de "Lazarillo" en la dura tarea de ser padres y madres de unos hijos e hijas totalmente conectados a todo tipo de dispositivos.

Es un hecho que Internet aporta a las nuevas generaciones grandes beneficios y oportunidades: comunicación, información, ocio, conocimiento... Sin embargo, los adultos hemos de ser conscientes de que también conlleva sus riesgos que, en ocasiones, pueden tener graves consecuencias.

Los escenarios en los que se mueven nuestros menores han cambiado, en cuanto a Tecnología se refiere. Tenemos que olvidarnos de las unidades estáticas, más fácilmente controladas, como puede ser el ordenador. Tenemos que empezar a poner énfasis en la conectividad móvil, la que les permite estar conectados a todas las horas y en todos los lugares. Por ello, para evitar riesgos en la red hay que educar y trabajar los valores, si no estamos perdidos ante una realidad tan difícilmente abarcable.

¿Qué tenemos que hacer?

Nos debemos ocupar. Es parte de nuestra obligación como personas adultas responsables de la protección y educación de los menores. La preocupación no sirve como nada. tampoco es útil desentenderse alegando confianza en el menor o incapacidad para ejercer esta tutela. Máxime cuando cuentan cada vez con más medios tecnológicos y a edades más tempranas.

Objetivos de la Guía

- Informar a las familias sobre los usos que sus hijos e hijas hacen de las Tecnologías.
- Potenciar el uso de las Tecnologías como elemento integrador y de desarrollo para ellos.
- Informar sobre los riesgos a los que están expuestos los menores.
- Sensibilizar de la importancia de trabajar en líneas de prevención sobre estos temas.
- Dar pautas de actuación a los progenitores en relación al buen uso de las Tecnologías.

¿CUÁNDO EMPEZAR A OCUPARNOS?

¿Has visto algo así por tu casa?

Si la respuesta es sí, es el

momento de empezar a

ocuparte, más que a

preocuparte



Con esta guía pretendemos que no os sintáis solos, que entendáis como normal el uso saludable que vuestros hijos hagan de las Tecnologías, entendiendo como saludable un uso sin abuso, con respeto y responsabilidad.

Puede que os encontréis en alguno de estos casos:

Que seáis unos padres "semidesconectados", y que dejan hacer a sus hijos lo que desean





- O bien unos padres "desconectados", que viven con cierta angustia la conexión de sus hijos.
- O miráis para otro lado.
- O tal vez sois unos padres "hiperpreocupados"...

En cualquier caso y seamos como seamos, los adultos sólo podemos trabajar en una línea, **la educación**. Será la única forma de prevenir los posibles contratiempos que puedan surgir de un uso incorrecto de Internet y de las Tecnologías de la comunicación.

¿TENEMOS LA FÓRMULA MÁGICA?

Lamentamos decirte que no y que tendrás que seguir leyendo.

A día de hoy y con unos entornos tecnológicos tan cambiantes en cuanto a dispositivos y aplicaciones, no existen las fórmulas mágicas. Pero sí que vamos conociendo qué es lo que da mejores resultados. La prevención, mediante la información y la educación, y más concretamente en valores.

En el ámbito de las Tecnologías al igual que en el resto de los campos que podamos relacionar con nuestros menores, la educación es fundamental para que sepan enfrentarse a un entorno que les permite mostrarse, crear, intercambiar y comunicar y hacerlo todo ello desde el Respeto y la Responsabilidad, las dos "R" imprescindibles para funcionar por Internet y no tener problemas.

Estamos dando paso al fin de una era en la que proteger los ordenadores que nuestros hijos utilizaban con un filtro, parecía suficiente para mantenerlos a salvo. Esto con la Tecnología móvil está cambiando. Nuestros hijos e hijas se conectan en cualquier lugar a cualquier hora y con cualquier dispositivo ya sea fijo o móvil.

Por todo esto es importante centrarnos en su educación, en proteger su integridad desde dentro con el fin de transmitirles unos valores e informaciones que les resulten útiles para sacar el máximo rendimiento de las herramientas que tienen a su alcance y que tantos beneficios les pueden aportar.

Como adultos debemos dejar e incluso fomentar que nuestros menores hagan uso de las tecnologías, pero nunca haciendo dejación de nuestras funciones como personas responsables del crecimiento de nuestros hijos e hijas. Hay que acompañarles y aconsejarles, ya que las Tecnologías no están exentas de riesgos, que hay que conocer para poder minimizarlos.



FOMENTO DE VALORES

Haremos hincapié en trabajar en la línea de la prevención desde todos los ámbitos relacionados con la educación de los menores, empezando por la propia familia. Solamente adoptando actitudes preventivas evitaremos acciones que perjudiquen al menor y, por extensión, a todo el núcleo familiar.

Dos son los valores que consideramos fundamentales para una navegación sin problemas en Internet, sea desde el dispositivo que sea: ordenador, Tablet o Smartphone.

Respeto

El **respeto** es el valor que permite que el ser humano pueda reconocer, aceptar, apreciar y valorar las cualidades de otras personas y las suyas propias. Es decir el respeto es el reconocimiento del valor propio y de los derechos de los individuos y la sociedad.

Respeto hacia los demás;

Por tanto es imprescindible que los menores aprendan a respetar a los demás, en los ambientes tecnológicos.

- Nespetando las opiniones de los demás en los foros, redes sociales, grupos de WhatsApp, etc.
- Nespetando la integridad moral de los demás evitando insultos y calumnias.
- Nespetando la propiedad de los demás, evitando las suplantaciones de identidad, robos de contraseñas y cuentas.
- Nespetando los datos personales de los demás, evitando subir fotos y videos de terceras personas, y más cuando les pudieran perjudicar.

Respeto hacia ellos mismos;

Y como el respeto empieza por uno mismo no está de más enseñar a nuestros menores a valorarse en la vida y entornos tecnológicos:

- Nespetando su integridad moral, evitando subir a Internet o enviar contenidos que les puedan perjudicar. Primer paso para prevenir el sexting (envío de contenidos eróticos o pornográficos por medio de teléfonos móviles).
- Nespetando sus datos personales, por ejemplo evitando subir fotos y videos con contenidos poco recomendables, evitarán problemas en un futuro cuando busquen trabajo o en el día de hoy si los ven sus padres o profesores.
- Si evitan dar muchos datos personales conseguirán mantenerse protegidos ellos y su familia.

Responsabilidad

La **responsabilidad** es un valor que está en la conciencia de la persona, que le permite reflexionar, administrar, orientar y valorar las consecuencias de sus actos.

Si aplicamos este concepto a las nuevas Tecnologías lo encontraremos como un valor imprescindible para el uso de las mismas. Si fomentamos este valor en los menores desde que comienzan con sus primeras navegaciones, adoptarán una actitud reflexiva, orientada a valorar las consecuencias de las acciones que realicen en sus servicios de Internet.

Así, por ejemplo, si un menor encuentra una sesión de Twitter abierta de un compañero, su primera intención puede ser gastarle una broma haciéndose pasar por él poniendo un tuit ofensivo para sus contactos. Pero, si su sentido de la responsabilidad lo tiene más o menos desarrollado, pensará "¿qué me puede pasar si hago esto? ¿y a mi compañero?" Para acto seguido cerrar la sesión de Twitter de su amigo de la manera adecuada, evitándose problemas a sí mismo y a su compañero.

Recuerda hijo mío:
Internet has de usar con
Respeto y Responsabilidad,
si un disgusto nos quieres
evitar

¿CUÁLES SON LOS RIESGOS?

A continuación detallaremos los riesgos que podemos encontrar en Internet.

Uso abusivo

Somos los padres y madres como adultos, los que debemos controlar los comportamientos anómalos en nuestros menores, si presentan ansiedad ante la imposibilidad de conexión, si dejan de hacer sus tareas habituales, si se vuelven irascibles en caso de no poder conectarse en un fin de semana (imaginad si vais de vacaciones), etc.

Tenemos que tener en cuenta que con los dispositivos móviles y sus aplicaciones los menores experimentan la necesidad de mantenerse casi continuamente conectados, ya que su grupo de iguales está ahí y, al contrario de lo que nos parezca a los adultos, experimentan el aislamiento social ante la ausencia de conexión.

El reto educativo consiste en enseñar a los niños y adolescentes a utilizar los dispositivos de una forma moderada. Muchos de ellos se sienten obligados a responder al momento de recibir un mensaje, y por ello, se sienten mal si no están continuamente conectados. En este punto es importante hacerles comprender que la mayoría de cosas pueden esperar.

Es importante negociar con nuestros hijos e hijas el tiempo de uso de las pantallas de las que hacen uso. Podéis encontrar más información en www.tecnoadicciones.com * de la Asociación Protégeles.

Acceso a contenidos inapropiados

A través de la red los menores pueden acceder a páginas web con contenidos no adecuados. Este es el riesgo en origen, el que siempre nos ha preocupado a padres y madres desde los inicios de Internet. ¿Qué verán mis hijos en Internet? ¿sexo? ¿violencia? ¿juegos de apuestas?... Ante este problema que nos podemos encontrar, existen algunas soluciones, como la instalación de filtros de contenidos. Aunque un filtro protege el ordenador de casa, pero no el del móvil, el de casa del amigo, el de la biblioteca, y además, no de todos los contenidos. Por ello seguimos apostando por la educación como prevención para evitar que nuestros hijos/as accedan a páginas no apropiadas para ellos/as.

^{*} En todos los enlaces a páginas Web: Pulsar Control + Enter para abrir el hipervínculo en otra pestaña del navegador de Internet.

Vulneración de los derechos de propiedad intelectual

Tenemos la obligación de informar a nuestros menores de que no todo el contenido que encontramos en Internet es de libre uso, ya que puede contener derechos de propiedad intelectual pertenecientes a su autor. Es decir, pueden encontrar una fotografía y utilizarla como si fuera suya pero sólo las que son de uso libre. Para ello existen páginas con recursos libres que podemos utilizar.

Acoso sexual o 'Grooming'

Se llama **Grooming** a las acciones deliberadas, realizadas por una persona adulta para establecer lazos de amistad con un niño o niña en Internet, con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual, posiblemente efectuado por medio de abusos contra los niños y niñas.

Se estima que el adulto en dos meses se gana la confianza del menor y es capaz de quedar físicamente con él.

En esta página www.quenoteladen.com se puede obtener una información más amplia de este tipo de delito, además contempla la posibilidad de utilizarla como herramienta para denunciar estas prácticas.

Amenazas a la privacidad. Por ejemplo 'sexting'

Con el uso de las redes sociales, los dispositivos móviles y sus aplicaciones, nos estamos exponiendo públicamente cada vez más. Estamos asistiendo a la pérdida de nuestra privacidad, compartiendo (consciente o inconscientemente), desde nuestros datos personales (nombre, apellidos, dirección, números de teléfono, fotografías, vídeos) hasta nuestros usos, costumbres o rutinas.

Ya no sólo estamos dejando ver lo que nosotros publicamos de nosotros mismos, sino también lo que los demás publican de nosotros o lo que nosotros publicamos de terceras personas.

Una de las formas más graves de amenaza a la privacidad que están sufriendo en estos momentos algunos jóvenes es el Sexting que consiste en el envío de fotos y videos con contenido sexual, producidos generalmente por el propio remitente, a otras personas por medio de teléfonos móviles y redes sociales, y que luego posiblemente terceras personas se encargarán de distribuir.

Delitos económicos y fraudes

Al utilizar las Tecnologías para realizar operaciones financieras estamos expuestos a riesgos si no tomamos las precauciones oportunas, como utilizar ordenadores con antivirus actualizados, tener los sistemas operativos actualizados, entrar en las páginas seguras de plataformas bancarias, etc.

Tenemos que pensar que hay personas que quizás estén esperando recoger nuestros datos y practicar el denominado **Phishing**, delito encuadrado dentro del ámbito de las estafas , y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. Una vez consiguen la información la utilizan para extraer dinero de nuestras cuentas bancarias.

El fraude tiene dos consecuencias directas sobre los usuarios: en primer lugar, la pérdida económica tangible en caso de que el ciberdelincuente consiga su propósito; en segundo lugar, la posible pérdida de confianza que podemos experimentar tras ser víctimas de una situación de fraude, que nos llevará, por ejemplo, a prescindir de realizar operaciones bancarias online para volver a realizar nuestras gestiones de forma presencial en el banco.



Rjesgos técnicos

El uso de las Tecnologías conlleva unos riesgos técnicos (pérdida de información, mal funcionamiento, robo de datos), que puede sufrir nuestro ordenador si no lo protegemos correctamente, así que siempre hay que tener el ordenador protegido con un antivirus

actualizado. Pueden descargarse antivirus gratuitos pero sólo de páginas fiables como: www.osi.es/recursos/utiles-gratuitos, Web dependiente del INCIBE, Instituto Nacional de Tecnologías de la Comunicación.

Ciberbullying

Se conoce Ciberbullying al acoso escolar entre iguales ejercido con medios digitales. Se considera más peligroso que el acoso propiamente dicho, ya que el chico/a que es acosado no descansa del acoso ni en el espacio ni en el tiempo. Sufre la agresión a todas horas, no sólo en horario escolar, y en todos los lugares, ya que la Tecnología accede a hogares, lugares de ocio y centros escolares.

Como padres y madres debemos estar atentos por si nuestros hijos pudieran estar sufriendo acoso, y ante un posible caso de acoso en la red o a través del teléfono móvil es imprescindible atajarlo lo antes posible y minimizar los efectos sobre la víctima.

Es de gran ayuda guardar las pruebas de la ciberagresión como son los mensajes SMS o correos enviados al acosado, además de informar al centro educativo e intentar recibir apoyo y asesoramiento de los psicopedagogos, y denunciarlo a la policía cuando así se valore.

Una vez confirmado que se está produciendo un caso de acoso, es necesario adoptar medidas drásticas; en primer lugar, se deberá cambiar la cuenta de correo electrónico y bloquear la dirección origen del acoso, así como el número de móvil, teniendo cuidado en no difundir los nuevos datos.

Respecto a los hijos es muy importante que se sientan apoyados y hacerles saber que están a su lado y que juntos serán capaces de superarlo. Una vez controlada la situación será el momento de hablar con los menores e incidir en las formas de evitar y prevenir estas situaciones.

Y el mayor **Riesgo**.... Ante una incidencia de seguridad:



LOS MENORES SE CALLAN

Como personas adultas no nos queda otra opción que intentar ofrecer a nuestros hijos e hijas un entorno de comunicación y confianza para que ante cualquier problema sean capaces de hablar con nosotros, porque, aunque no sepamos mucho de Tecnología, de la vida sabemos más y siempre podemos ayudarlos ante cualquier problema.

Y AHORA... ¿QUÉ HACEMOS?

Podemos aplicar una serie de recomendaciones que harán de las Tecnologías una herramienta positiva para el desarrollo de nuestros hijos e hijas



Recomendaciones generales cuando tengo una conexión a Internet

Tenemos que partir de una base, los problemas no los generan los dispositivos ni las conexiones a Internet. Los problemas son generados por las personas que los usan, que son los que dan el alma a las herramientas utilizadas.

Además, pensemos que hay una serie de normas que nuestros menores deben asumir desde que tienen sus primeros coqueteos con las Tecnologías, y más cuando el acceso cada vez se establece antes, en torno a los 2 y 3 años según el estudio realizado por la entidad Protégeles: "Esta nueva situación plantea una verdadera oportunidad. Ya que el acceso de los menores a Internet, en edades cercanas a los 13-14 años, ha hecho muy difícil hasta ahora la interacción entre padres e hijos en relación a las Tecnologías. Los adolescentes de dichas edades son muy reacios a permitir que sus padres accedan a su perfiles en las redes sociales, les aconsejen sobre sus conversaciones, o vean las fotos que van a colgar antes de que las publiquen. Durante la adolescencia el peso del grupo de iguales es cada vez mayor, y el distanciamiento de los padres se hace notable. La conectividad móvil, al bajar tanto la edad de inicio, está permitiendo que accedan a Internet y las TIC en general niños y niñas muy pequeños. Los menores de estas edades, interactúan mucho con sus padres, y son especialmente receptivos a los consejos y recomendaciones de sus mayores. Aprenden mucho mediante el juego, y además les gusta jugar con sus mayores, mostrarles lo que saben hacer, lo que han descubierto, el video que han visto o el nivel que han alcanzado en determinado juego. Así pues, los nuevos terminales móviles permiten a los padres de los niños más pequeños realizar una verdadera labor educativa. Sentarse con ellos, practicar e incluso aprender a su lado, permitirá iniciarles en el manejo de las TIC como si de un juego se tratase, abordando cuestiones como el tipo de fotos, la privacidad, el respeto a los demás, y otras de forma natural y sin conflicto".

Veamos entonces qué recomendaciones conviene aplicar en el hogar desde sus primeras conexiones:

1. Pongámonos al día con las Tecnologías.

Como madres y padres preocupados no nos queda otra opción que ponernos manos a la obra y empezar a entender el mundo en el que se mueven nuestros hijos. Si no tenemos ningún conocimiento sobre ordenadores, es una buena idea comenzar formándonos con un curso básico, y si, por el contrario, estamos habituados a su uso, pero se nos escapan términos que ahora están muy de moda, podemos incluso pedirles a nuestros hijos e hijas que nos expliquen en qué consiste" eso de WhatsApp", Twitter, Instagram, Facebook, YouTube..." Son palabras adquiridas en la rutina diaria de los menores y que al compartir su significado y utilización con nosotros, nos ayudará a establecer un acercamiento hacia ellos.

2. Normas claras desde la primera conexión

Como hemos dicho, cuanto antes empecemos a educar en el uso de las Tecnologías a nuestros hijos, más eficaz será la prevención que ejerzamos sobre ellos. Para ello tienen que percibir que los padres y madres tenemos muy claro cómo hacer uso de las Tecnologías, que aplicamos y recordamos las normas básicas para manejarse en Internet, desde que un dispositivo entra en casa, ya sea fijo o móvil. Por ejemplo, el mismo día de la compra del teléfono móvil podéis firmar un contrato en el que se especifique varios asuntos como: horarios de uso, descarga de aplicaciones, comportamiento, etc.

3. Control del espacio físico que ocupan los dispositivos

Por ejemplo, pondremos el ordenador fijo en un lugar común de la vivienda como el salón o la habitación en la que habitualmente permanezca la familia, de esta manera ejerceremos un control sin que los menores se sientan invadidos, y, así, evitaremos que se lleven a cabo acciones que puedan ser reprobadas por los padres y madres.

Los dispositivos móviles, tanto Tablet como Smartphone permanecerán en un espacio de la casa preparado para su carga, durante la noche, hora de los deberes, y hora de las comidas. Este lugar puede denominarse *parking móvil*.

Por otro lado, es importante, si el ordenador está en la habitación de los menores, que la pantalla mire hacia la puerta y esta permanezca abierta. Nunca jamás la pantalla deberá dar la espalda a la puerta.

4. Limitemos los tiempos de uso

Como en todos los aspectos de la vida que rodean a nuestros hijos hay que controlar el tiempo que dedican a la televisión, videojuegos, deportes o estudios. Las Tecnologías no son un asunto aparte, y corresponde a las familias determinar el tiempo dedicado al ocio y comunicación por Internet.

Una buena forma de limitar el tiempo de uso del móvil es utilizando el parking de móviles.

5. Poner contraseñas para la descarga de aplicaciones

Active una contraseña en el dispositivo móvil tanto Tablet como Smartphone para controlar la descarga de aplicaciones o la realización de compras. Sólo usted debe conocer dicha contraseña.

6. Tengamos los dispositivos fijos y móviles protegidos con una solución de seguridad (antivirus, cortafuegos)

Para no resultar perjudicados por un mal uso de Internet es importante mantener nuestros sistemas protegidos con soluciones de seguridad integrales, esto no requiere ni de grandes conocimientos ni grandes inversiones, es más, podemos encontrar herramientas de protección gratuitas en la siguiente dirección: www.osi.es/recursos/utiles-gratuitos.

Además de tener una solución de seguridad es imprescindible mantener los sistemas operativos actualizados.

7. Instalar filtros de contenido en los dispositivos con conexión.

Es recomendable instalar en los ordenadores y móviles de la vivienda unos filtros de contenidos, tal como veremos en el apartado "recomendaciones sobre contenidos", aunque debemos ser conscientes de que la instalación de un filtro no nos deja exentos de tutelar las navegaciones de nuestros hijos.

8. Crear cuentas de usuario separadas para sus hijos e hijas

Asegúrese de que los ajustes de privacidad estén en el nivel más alto (examine el menú "opciones" en su navegador).

9. Uso racional de la Webcam

La webcam es una herramienta útil para la comunicación y atendiendo a una serie de normas no tiene por qué darnos problemas. Las normas son claras: cuando la webcam no esté siendo utilizada, y aunque los dispositivos estén apagados, tiene que estar mirando al techo, a la

pared o metida en un cajón, si es un dispositivo fijo, y si se trata de una Tablet o un Smartphone, un ordenador portátil, basta con poner sobre la cámara una pequeña pegatina. Los terminales con cámara no deben entrar en el cuarto de baño, o en aquellos sitios en los que el menor vaya a permanecer con la puerta cerrada.

Estas son medidas de seguridad porque existe la posibilidad de que ante un mal uso hecho por nuestra parte (por no tener antivirus, abrir archivos que no debemos...)

se pueda instalar un archivo espía que active grabaciones dentro del hogar (en el dormitorio, baño, etc.) de contenido comprometido y que puedan ser objeto de chantaje hacia los miembros de la familia.

Además hay que insistir a nuestros hijos en que tan solo utilicen la Webcam con gente de máxima confianza y en momentos puntuales.

10. Acompañemos a nuestros hijos e hijas en sus navegaciones

No nos sirve de nada preocuparnos si no somos capaces de ocuparnos de las actividades que nuestros hijos/as realizan en Internet. Es interesante acompañar a los menores en sus búsquedas por ese ilimitado mundo de Internet. No podemos dejar que ellos realicen sus búsquedas sin nuestra supervisión. Pongamos un ejemplo: nuestro hijo/a quiere buscar un juego de coches en Internet, nosotros como adultos le acompañaremos en su búsqueda. Si la página encontrada nos parece correcta, y el juego también, podremos dejarle jugar recordándole que, si quiere cambiar de juego, nos tendrá que avisar.

Ante una incidencia de seguridad acude a entidades especializadas

En primer lugar, debemos recordar que contamos con las entidades implicadas en el crecimiento de nuestros hijos como pueden ser los centros escolares, los cuales nos pueden dar alguna pauta de actuación.

Asimismo, tenemos que saber que existen entidades que se dedican de forma específica a la protección del menor en Internet como es www.protegeles.es o www.fundaciondedalo.org páginas especializadas además, en Nuevas Tecnologías.

Ante cualquier incidencia de seguridad (*ciberbullying*, acoso, insultos, suplantación de identidad, etc) que tengáis con vuestros hijos e hijas, todos ellos pueden ayudaros.

Recomendaciones sobre contenidos

La búsqueda de contenidos en la Red es el uso más frecuente y habitual. Utilizamos esta herramienta como un lugar en el que lo encontramos todo: para ocio, comunicación, o trabajo. Para ello existen potentes buscadores que nos ayudan a llegar donde nos hemos propuesto, el más utilizado en estos momentos es Google. No obstante, debemos fomentar el espíritu crítico y selectivo ante los buscadores. Y en muchas ocasiones confundimos la barra del buscador instalada en el navegador o toolbar (indicada con un 2 en la imagen) con la propia barra de direcciones del navegador (indicada con un 1 en la imagen).



Ejemplo de barra de direcciones (1) y barra de Google (2)

Deberíamos acostumbrar a nuestros hijos a buscar desde la barra de direcciones en caso de que tengan el nombre de la página web en la que quieren entrar. De esta forma evitaremos que se distraigan con otras muchas páginas que les indiquen desde el buscador.

Existen herramientas que van a facilitar la vida de los progenitores en cuanto a contenidos se refiere, siempre y cuando nuestros hijos sean menores de aproximadamente 10-11 años. Estas herramientas, que pueden ser aplicadas en dispositivos fijos y móviles, actúan como filtro de contenido:

Navegadores infantiles

www.kidoz.net



Buscadores infantiles

www.buscadorinfantil.com

www.kidrex.org



YouTube Kids



También podemos buscar recursos dirigidos específicamente para menores, como este nuevo canal de Youtube para ver videos. Esta aplicación gratuita, que se puede descargar para móvil, ordenador o tablet, es una recopilación de vídeos, canales y listas de reproducción adecuados a la edad.

Asimismo, tenemos la posibilidad de **Activar los filtros de Google** que te permiten cambiar la configuración del navegador para evitar que aparezca contenido para adultos en los resultados de búsqueda. Google utiliza métodos automatizados para identificar contenido ofensivo. En el caso de contenido sexualmente explícito, este filtro se basa principalmente en algoritmos que

tienen en cuenta diversos factores, incluidos enlaces, palabras clave e imágenes. Ningún filtro es fiable al 100%, pero **SafeSearch** puede ayudarte a excluir la mayor parte de este tipo de contenido.

Además de las opciones anteriores desde la página www.osi.es/es/recursos/utiles-gratuitos podemos acceder a controles parentales gratuitos.

Concluimos este capítulo haciendo hincapié en la necesidad de la **educación** por encima de cualquier herramienta que nos permita controlar el uso de las acciones que nuestros hijos realizan en Internet, ya que estamos asistiendo a las primeras generaciones de conectados móviles. Es decir, que ya no solo se conectan en casa (a través de ordenadores de mesa) sino que tienen móviles con conexión a Internet (Smartphone) con lo cual su conexión se realiza desde cualquier lugar, ampliando la disponibilidad de Internet.

Recomendaciones sobre los registros en los servicios de Internet

Otro gran uso que realizamos en Internet es buscar aplicaciones, servicios y plataformas que nos permita relacionarnos, comunicarnos, pasar ratos de ocio, etc. Redes sociales, páginas de compras online, foros, chats, correos electrónicos, entre otras, son "realidades virtuales" a las que accedemos habitualmente, nosotros y nuestros hijos. Para utilizar todos estos servicios es totalmente necesario realizar un registro en las mismas, sabiendo que cualquier registro requiere de proveer a esas plataformas de todos nuestros datos personales: Nombre apellidos, correos electrónicos, fechas de nacimiento, teléfonos, lugar de residencia, gustos y aficiones, fotografías.

La primera premisa para padres y madres en Internet debe ser que 'Los menores de 14 años no pueden dar sus datos personales en Internet', así pues si nuestros hijos e hijas necesitan registrarse en algún servicio nos lo tendrán que comunicar y seremos los adultos los que introduzcamos nuestros datos personales donde sean requeridos.

Además de esto, serán varias las cosas que habrá que tener en cuenta al registrarnos:

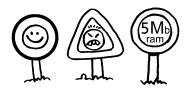
1. Elegir los servicios de Internet adecuados

Hay que ser conscientes de que todas las plataformas y servicios que nos ofrece Internet no son recomendables, así que hay que ayudar a nuestros hijos a utilizar los servicios más adecuados.

¿Cómo les ayudamos a elegir? Si como padres y madres se nos hace difícil saber seleccionar, podemos atender a una serie de recomendaciones:

- Aspecto físico de plataforma en la que quieren registrarse.
- En segundo lugar es importantísimo leer las condiciones generales de uso de todos los servicios de Internet en los que nos registramos ya sean redes sociales, correos

- electrónicos, páginas comerciales... En las condiciones nos avisan de aspectos importantes como los derechos de propiedad intelectual, edad de uso, leyes que los legislan y otros asuntos de importancia.
- Por último podemos buscar información por Internet e informarnos sobre las características de las plataformas y, por ejemplo, desechar aquellas que fomentan la comunicación anónima, tipo *Ask.fm*. O aquellas que permiten destruir mensajes en breves segundos ya que fomentan el intercambio de material comprometido, un ejemplo de estas puede ser, *Snapchat*. En definitiva, descartar todas aquellas que pongan en riesgo su privacidad. Atender a todas las señales que nos indiquen qué servicios son adecuados o no.



2. Atención a la hora de poner las contraseñas

Ya hemos decidido qué plataforma usar, así que vamos a registrarnos. En todo registro de Internet, nos solicitan para nuestra seguridad que introduzcamos una contraseña, la cual teclearemos para identificarnos cada vez que queramos acceder a ese servicio. En ocasiones no nos paramos a pensar ni le damos mucha importancia a estas contraseñas que utilizamos en nuestra vida cotidiana. El correo electrónico personal, el email del trabajo, la cuenta en Facebook, Instagram, la tarjeta de crédito, la alarma de casa, el PIN del móvil, etc. A las contraseñas hay que darles el valor que se merecen, ya que va a ser la herramienta que proteja nuestros servicios en la red.

Para ello hay unas medidas básicas que debemos tener en cuenta en cuanto al uso de contraseñas en Internet:

- Las contraseñas deben ser fuertes, es decir, de 8 caracteres alfanuméricos con mayúsculas y minúsculas, y con algún signo intermedio.
- Es conveniente tener una contraseña diferente para cada servicio en el que estemos registrados. Una para el correo electrónico, otra para las redes sociales, otra para el blog,... De esta forma si te descubren una evitarás que tengan acceso a todos tus servicios.
- Evita que los equipos recuerden tus nombres de usuario y contraseñas de forma automática. Es importante estar atentos ya que algunos servicios pueden tener configurado por defecto la opción de recordar la cuenta y la contraseña.
- ▶ Por último es muy importante cerrar las sesiones de la manera adecuada. Es decir, nunca se debe cerrar del aspa () sino desde dentro del servicio que estemos utilizando.



Recomendaciones sobre los servicios que utilizamos

Una vez elegidos los servicios y efectuado el registro, ya podemos empezar a manejarlos con los servicios y aplicaciones. Vamos a ver los más utilizados:

1. Correo Electrónico

El correo electrónico es desde hace más de una década la forma de comunicación por mensajes más extendida por la red, pero no es de extrañar que con la llegada e implantación de otros sistemas de comunicación el e-mail pierda protagonismo. Además, lo utilizamos como modo de registro de otros servicios.

Pasamos a detallar varias recomendaciones para evitar problemas con el uso del correo-e:

Hacer envíos a varios contactos con copia oculta (CCO). Si no lo hacemos así, estamos distribuyendo datos de terceras personas sin su consentimiento, siendo esto lo que se considera una infracción.



- ➤ También se considera recomendable filtrar el correo que pudiera ser considerado "Hoax" (mensajes de correo electrónico engañosos que se distribuyen en cadena).
- Tener más de una dirección de correo-e: personal, profesional y comercial.
- No abrir archivos adjuntos que no conocemos.

2. Redes sociales

Como ya hemos explicado las **redes sociales** son plataformas que permiten realizar múltiples actividades sin salir de la misma. Es por ello de gran utilización y utilidad para sus usuarios.

Encontramos gran variedad de redes sociales en estos momentos, muchas de ellas y las más conocidas tienen como fin la socialización e intercambio de contenidos, en esta clase podemos incluir las conocidas: *Facebook* y *Twitter*. Hay otras redes de entornos profesionales donde se agrupa gente para intercambiar y compartir sus perfiles profesionales, como *LinkedIn*. Tenemos las redes sociales temáticas de imágenes como *Instagram* y *Pinterest* que se están expandiendo cada vez más por su uso vinculado a otras como Twitter y por su utilidad como canal social.

Los usos y costumbres de los menores cambian a un ritmo exponencial, por ello no nos centraremos en ninguna plataforma ni servicio en concreto, sino que aportaremos unas pautas generales para el manejo de las plataformas sociales.

Recomendaciones para hacer un buen uso de las mismas. En relación a los menores hay que tener en cuenta varios aspectos importantísimos:

1. Control sobre edad de acceso y condiciones

Controlar la edad de uso de las redes sociales, por lo general, no tienen el acceso permitido a menores de 14 años. Para ello conviene leer las condiciones de uso. Por ejemplo WhatsApp es para mayores de 16 años.

2. Control de privacidad en redes sociales

Los padres y madres debemos controlar cómo tienen configurada la **privacidad** nuestros hijos e hijas, en cualquier plataforma que utilicen, por ejemplo en Twitter es muy habitual que tengan configurados los perfiles públicos, a través de los cuales, y con la navegación frecuente, construyen con lo que hacen un diario de su vida accesible a todos los públicos. Puede ayudarnos el siguiente enlace: www.deaquinopasas.org



3. Control de sus contactos

Por otro lado, hay que estar al día de los **contactos** que tienen en las redes sociales. Esto es importantísimo para prevenir el *Grooming* (acoso de un adulto a un menor).

Nuestro mensaje que transmitir a los menores debe ser claro:

- Que tengan en las redes sociales los mismos amigos que tienen en la vida real.
 Resulta una práctica útil repasar con nuestros hijos sus listas de contactos, e ir eliminando aquellos que no conocen físicamente.
- Animarles a rechazar invitaciones de contactos que no conocen, que no duden a la hora de bloquear ni quitar un contacto.
- Y por supuesto que nunca queden con alguien que no conocen.

Como adultos responsables debemos insistir en que:

> En las redes sociales comparto información sin afectar mi intimidad, ni la de otros.

- Respeto la información que tengo de las personas que conozco y no la publico sin su autorización en las redes sociales.
- No publico nada que un futuro me pueda comprometer.

4. Control sobre las imágenes subidas a redes sociales

La red social Facebook anunció que ya almacena a diario más de 250 millones de imágenes, el equivalente a cinco fotografías subidas a diario por cada habitante en España. Google+, la nueva red social de Google dijo que ya almacenan 3,4 millones de fotos en 100 días.

Hablando de estas cifras debemos mencionar las precauciones que deben tomar los menores

a la hora de compartir una fotografía o un video.

Aspectos que debes tener en cuenta con las fotos y vídeos:

Evitar subir o enviar material comprometido;

Es inevitable que los usuarios de redes sociales suban fotografías a Internet, ya que es una forma rápida, cómoda y eficaz de compartirlas. Ahora bien, como padres y madres sería conveniente retrasar lo más posible el compartir fotos y videos donde los protagonistas sean los menores.

En Internet hay
que pensar en años
no en minutos



Hay que ser conscientes de que no deben subir nada a la red que les pueda perjudicar en un presente o en un futuro.

Hoy en día cada vez los menores cuentan con más materiales gráficos, ya que llevan móviles con cámaras de fotos, lo cual les permite hacer registro de todo lo que hacen. Imaginemos un adolescente que sale de botellón, bebe más de la cuenta y sus amigos le inmortalizan en unas fotos que más tarde suben a Internet y las comparten con el resto de sus amigos. Esa foto ya queda en Internet y quizás pueda ser vista por padres, profesores..., a la larga y en un futuro por el responsable de recursos humanos de la empresa que le va a contratar.

Mención especial merece el riesgo del **sexting**, que ya hemos mencionado, que consiste en el envío a otras personas, de fotos y videos con contenido sexual producidos generalmente por el propio remitente, por medio de teléfonos móviles y redes sociales, y que luego posiblemente terceras personas se encargarán de distribuir. Hay que insistir a los menores que no envíen fotografías que no quieren que se vean públicamente.

Las fotos se pueden descargar;

Cualquier foto subida a Internet puede ser descargada. Aunque hay redes sociales que dan la opción de no dejar descargar, la realidad es que cualquier imagen que aparece en la pantalla de un ordenador se puede capturar tan fácilmente como con la tecla "imprimir pantalla", o con una simple fotografía de la misma.



Insistimos en la importancia de alertar a los menores del uso de aplicaciones que fomentan la destrucción de material, en estos momentos tipo *Snapchat*, ya que favorecen la difusión de material comprometido.

Las fotos y videos necesitan autorización de las personas que salen en ellas;

La Agencia Española de Protección de Datos (AEPD) reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos. Si contamos con que las fotos y videos son datos personales tenemos el derecho de decidir si los publicamos o no y de que nadie los publique sin nuestro consentimiento. Y al contrario, tenemos la obligación de proteger la información de los demás. Por ello no podremos publicar fotos y videos sin su consentimiento.

- Podemos ser responsables por daños causados a la imagen, reputación o intimidad de otras personas
- Los datos personales que se publican en Internet disponibles para cualquiera pueden escapar a nuestro control y ser muy difíciles de eliminar con posterioridad.
- Podemos poner en situación de riesgo a otras personas, especialmente cuando se trate de imágenes de menores
- Internet es un medio con características muy específicas: lo que en el mundo físico puede no ser más que una broma de mal gusto en Internet puede causar graves perjuicios.

Para ampliar información es muy recomendable consultar la documentación de la AEPD:

Recomendaciones a usuarios de Internet:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_recomendaciones_internet_052009.pdf

Guía Derechos de niños y niñas, deberes de padres y madres, destinada a los menores: www.agpd.es/portalwebAGPD/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf

Una foto en Internet es incontrolable;

Cuando una foto sale de cualquier dispositivo es imposible de controlar, ya que queda a disposición y arbitrio de todos los usuarios de Internet que tengan acceso a ella. Aunque pretendamos borrarla una vez enviada o subida a una plataforma, es tarea imposible de cumplir.

Recomendaciones sobre teléfonos inteligentes (smartphones)

Con la aparición de los nuevos teléfonos inteligentes o **Smartphones**, la conexión a Internet ha pasado a ser móvil, con lo que como padres debemos ocuparnos también de tutelar esos pequeños dispositivos que han entrado en nuestros hogares y son capaces de conectar a nuestros hijos e hijas con el resto del mundo.



Los riesgos a los que se enfrentan nuestros hijos con el uso de Smartphone son los mismos que estamos detallando a lo largo de

esta guía: uso excesivo, dependencia, amenazas a la privacidad, acceso a contenidos inapropiados, *sexting*, *grooming*, *ciberbullying*,... Aunque todos ellos agravados por la alta disponibilidad de estos dispositivos, en tiempo y en espacio. Además de ser, por sus características los aliados de la inmediatez y la falta de reflexión.

Para ampliar esta información podemos leer el estudio publicado por la Asociación Protégeles sobre *Menores de edad y conectividad Móvil en España: Tablets y Smartphones.*www.diaInternetsegura.es/descargas/estudio_movil_smartphones_tablets_v2c.pdf

1. Uso del Smartphone

Tendremos en cuenta varios aspectos:

- Tutelar la compra del Smartphone. Lo ideal es que los padres supervisen el proceso de compra del teléfono, así como de otras herramientas de comunicación electrónicas. Es importante que os informéis de los servicios que ofrecen y cómo manejarlos.
- El teléfono prepago puede ser la manera de controlar el gasto y limitar su uso. Aunque cada vez proliferan más los packs familiares, que salen más económicos. En este caso conviene estar atentos a las condiciones de contrato, por ejemplo, que no sean ampliables las tarifas de datos sin nuestro consentimiento.
- Pactar normas de uso, mediante la firma de un contrato o similar, entre padres e hijos a la compra de un dispositivo (tiempo, gasto mensual y servicios), evitando el uso abusivo o dependencia del teléfono móvil.
- Uso de un parking para móviles. Preparar en casa un espacio en el que dejar los móviles en momentos determinados de la jornada, como la noche, las horas de las tareas o las horas de comer. Podemos aprovechar para que sea el lugar en el que pongamos a cargar los móviles.
- Mantener el Smartphone protegido con contraseña, para evitar posibles incidentes en caso de pérdida del dispositivo.

Smartphone no deja de ser un ordenador en miniatura, con lo que no está de más volver a recordar a nuestros hijos una serie de normas importantes como: "cuidado con los contenidos que publicas en la Red", puesto que en Internet todo lo que se publica se mueve a gran velocidad y no sabemos a dónde puede llegar. Internet móvil permite una mayor rapidez tanto en la publicación de "lo que está pasando" como en la "viralidad" de difusión del contenido. Es preciso recordarles la importancia de su privacidad y los riesgos que pueden derivar de compartir información con desconocidos.



- Ojo con el servicio de geolocalización que indica la ubicación del portador del teléfono móvil y es un servicio que viene, por defecto, conectado. No es aconsejable que todo el mundo conozca el paradero de tu hijo o hija. Por ello recomendamos conocer bien la forma de uso y la funcionalidad del servicio de geolocalización y ser conscientes de que cada vez que se publica algo en una red social desde un teléfono con el servicio activado, todas las personas que ven la publicación pueden saber exactamente desde dónde fue realizada.
- Mantener desactivado el bluetooth y otras vías de entrada de contacto que no se usen con frecuencia. Es recomendable mantenerlas desconectadas para minimizar riesgos de virus y otros agentes intrusivos.
- Controlar la sincronización automática para realizar copias de seguridad, por ejemplo en los dispositivos con sistema Android, hay que tener mucho cuidado al sincronizar las fotos realizadas a Google+ donde se realiza la copia de seguridad. Conviene revisar las condiciones de privacidad de la plataforma en la que se descargan las imágenes.
- **Que no se callen**, ante cualquier acontecimiento que les incomode a través de sus smartphones, ante una foto inapropiada, un insulto o una ofensa.

2. Servicios de mensajería instantánea: WhatsApp



Vamos a hacer una mención especial a *WhatsApp*, la aplicación multiplataforma líder de mensajería para los Smartphones. La aplicación ha conseguido que los usuarios de dispositivos móviles estén conectados de forma gratuita, ya que permite mantener conversaciones sin necesidad de pagar por los mensajes enviados.

Además también se puede intercambiar imágenes ilimitadas, vídeo y audio. Por ello tiene millones de adeptos también entre los adolescentes.

Una característica de WhatsApp es que absorbe de forma automática todos los contactos que tenemos en el móvil que tienen esta aplicación instalada. Existen una serie de recomendaciones que hay que tener en cuenta:

- No usar nunca este servicio para mandar números de tarjetas de crédito, pins, cuentas bancarias.
- No usar WhatsApp para mandar material "sensible". Evita el sexting.
- → Hacer un uso responsable de la aplicación. Controlar los usuarios que tienen acceso a nuestro WhatsApp y ser responsable y respetuoso con el contenido que generamos en esta plataforma.
- Cuidado a la hora de enviar los mensajes. Evitar las prisas y confirmar que el destinatario es el que queremos. Asegúrate de que envías el mensaje a quien quieres hacerlo, hay confusiones en los destinatarios que pueden ser fatales para tu vida personal o profesional.
- ≥ En los Grupos hay que evitar los malos entendidos, utilizar los emoticones: si algo es una broma indicarlo con el emoticono adecuado (☺).
- Valorar por las familias si interesa llevar la última hora de conexión puesta. Es una forma de proteger la privacidad de los menores desconectar la hora de conexión. Se trata de una forma de control que debemos evitar.
- No abras todos los links que te envíen vía *WhatsApp* y desconfía de enlaces acortados, sobre todo si desconoces quién te lo manda. Ignórales y bloquéales.
- Suidado con las redes Wi-Fi que utilizas para enviar mensajes. Si no están debidamente protegidas o son Wi-Fi públicas, un delincuente o persona con malas intenciones podría capturar las conversaciones que intercambias con tus contactos.

 Suidado con las redes Wi-Fi que utilizas para enviar mensajes. Si no están debidamente protegidas o son Wi-Fi públicas, un delincuente o persona con malas intenciones podría capturar las conversaciones que intercambias con tus contactos.

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

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

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con las redes Wi-Fi que utilizas para enviar mensajes.

 Cuidado con la cuidado
- Atento a los mensajes en cadena o 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, en 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.



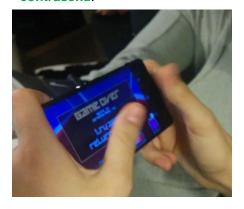
Recomendaciones sobre videojuegos

- Los padres debemos supervisar la compra o descarga de videojuegos, tarea fundamental para garantizar la seguridad. Debemos atender a las recomendaciones de los fabricantes según los códigos establecidos.
- Conviene colocar la consola o el ordenador en zonas comunes de la casa para evitar que el niño permanezca aislado, y así controlar su actividad.



- Intentar promover el juego en equipo con el niño o niña, organizando las partidas y los turnos de cada uno.
- Hay que controlar las horas de juego con los videojuegos. Jugar con videojuegos no debería interferir con otras actividades del niño. Por ello, es de gran importancia controlar el tiempo que dedica a los videojuegos. Se recomienda reducir los juegos a fin de semana y vacaciones. En el caso de jugar entre semana, el

- tiempo debería quedar limitado siempre y cuando los niños hayan terminado los deberes escolares y otras actividades que pudieran tener.
- Es recomendable intercalar el tiempo dedicado a jugar con los videojuegos y los tiempos de descanso.
- Concienciar a los menores sobre la importancia de la privacidad en los videojuegos y en la Red, tanto propia como del resto de personas de su entorno. Alértales sobre los riesgos existentes.
- Controlar los accesos a chats o juegos en línea con otras personas. Dejadles jugar sólo con usuarios y usuarias conocidos y que nunca den datos personales.
- Tener las cuentas para la compra de juegos y servicios a través de las consolas con usuario y contraseña.



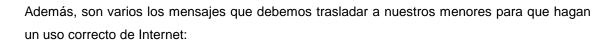
Recomendaciones para evitar tener problemas con la Ley

Como padres y madres tenemos que estar informados de que nuestros hijos pueden incurrir en faltas y delitos, en muchas ocasiones por falta de información, porque en muchas ocasiones traspasan la delgada línea que separa una broma de un delito. Tenemos que ser consciente de que tan malo es encontrarnos en la situación de ser padre o madre de un niño o niña víctima de acoso o de delito como serlo del menor ejecutor del mismo.

Los delitos y faltas más frecuentes entre menores son calumnias e injurias, suplantaciones de identidad, *ciberbullying* o faltas contra la intimidad.

Como padres y madres debemos saber que:

- Ser menor de edad no exime de responsabilidad. Es decir, que aunque seas menor eres responsable de lo que hagas.
- El desconocimiento de las leyes no exime del deber de cumplimiento de las mismas. Es decir, que no conozcas las leyes no quiere decir que no debas cumplirlas





Al navegar por Internet, aunque a priori puede parecer una acción anónima, se deja rastro. Cuando nos conectamos a Internet se nos asigna una dirección IP, que es un número que viene a ser como el nombre y apellido de nuestro ordenador al conectarse a la red. En el caso de que se cometa un delito o una falta y esta sea denunciada, las brigadas especializadas de la Policía tienen mecanismos más que suficientes para iniciar un rastreo y ver desde qué ordenador se ha cometido la falta.



2. Enseñarles a ser honestos con su edad

Es práctica habitual entre los menores engañar sobre la edad que tienen para poder registrarse en muchos de los servicios de Internet que tienen prohibido el acceso a menores de 14 años, que es la edad legal a partir de la cual el menor ya tiene derecho a decidir. Hasta esa edad seremos los padres y madres los que respondamos por ellos.



3. Evitar que los menores se hagan pasar por otros

Para evitar un delito de suplantación de identidad, el primer paso es concienciar a los menores de que adopten las medidas oportunas para no ser suplantados. Por un lado, deberán tener contraseñas fuertes y cerrar sus sesiones de la manera adecuada, además de no decir sus contraseñas a sus amistades. Por otro lado, deben evitar tentaciones de hacerse pasar por otros para gastarles una broma o saldar una cuenta pendiente. Si encuentran una sesión de Internet abierta (*Twitter*, *Instagram*, correo...), tienen que cerrarla.

4. Informar a los menores de que un insulto les puede meter en un lío

Los insultos, injurias y calumnias al igual que la suplantación de identidad pueden llegar a convertirse

en delito. Por ello es importante incidir en la necesidad de que los menores actúen con respeto en Internet y redes sociales, sin agredir la integridad de los demás, que actúen como la hacen en la "vida real", en el "cara a cara", porque lo que es un delito en la calle lo es también en Internet.

CONCLUSIONES

Como conclusión es conveniente resaltar un par de cuestiones que consideramos esenciales:

Generar Clima de confianza y Fomento de valores

Por un lado sólo nos queda generar en casa un clima de confianza por el que podamos saber de su vida digital, de manera que ante cualquier problema que se les presente sean capaces de contárnoslo y tomar las medidas oportunas.

Muchas veces esto se resuelve cuando nuestros hijos ven que comprendemos qué es eso de las Tecnologías: entendemos de WhatsApp, de Twitter y de etiquetas (hashtags), y que somos capaces de incorporarlo a nuestro lenguaje diario, en una cena o una comida. Es decir, que al igual que les preguntábamos "¿con quién has estado hoy en el parque?", les podamos preguntar ahora "¿con quién has hablado hoy en WhatsApp?" o "¿Has subido alguna foto a Instagram?"

Y por otro lado, tenemos que incidir en la necesidad del **fomento de valores** en nuestros menores, ya que si estos tienen unos valores y normas adquiridos para la vida, será difícil que hagan un mal uso de esta herramienta que es Internet.

Sólo nos queda animaros a seguir con vuestra difícil tarea educadora como padres y madres, y recalcar que las nuevas Tecnologías no dejan de ser una herramienta a nuestro servicio, que son una prolongación de lo que nosotros mismos somos y que nosotros les damos el alma a esas máquinas.

Fomentemos la parte positiva de Internet, que conecta a nuestros hijos e hijas con el Planeta Azul.



ANEXO

Imágenes de la Guía

- Imágenes página 2 _ Producidas por Ekilikua para Fundación Dédalo y Propias de Fundación Dédalo
- Imagen página 3_ Producidas por Ekilikua para Fundación Dédalo
- Imágenes 5 y 8 _ Producidas por Ekilikua para Fundación Dédalo
- Imagen página 9_ Imagen propiedad Fundación Dédalo
- Imagen página 10_ Producidas por Ekilikua para Fundación Dédalo
- Imágenes página 16_ Producidas por Ekilikua para Fundación Dédalo y captura de pantalla
- Imagen página 17_ Captura de pantalla
- Imagen página 18_ Captura de pantalla
- Imagen página 21 _ Imagen propiedad Fundación Dédalo
- Imagen página 22 _ Imagen propiedad Fundación Dédalo
- Imagen página 23_ Imagen propiedad Fundación Dédalo
- Imágenes página 24_ Imagen propiedad Fundación Dédalo
- Imagen página 25_ Imagen propiedad Fundación Dédalo
- Imágenes página 26_ Imagen propiedad Fundación Dédalo
- Imágenes página 27_ Producidas por Ekilikua para Fundación Dédalo

Fuentes y Bibliografía

- Estudio sobre hábitos seguros en el uso de las TIC por niños y adolescentes y econfianza de sus padres de Inteco, ahora INCIBE. https://www.incibe.es/CERT/guias_estudios/Estudios/Estudio_ninos
- Web de Tecno-adicciones www.tecnoadicciones.com de la Asociación Protégeles.
- Página de Protégeles www.quenoteladen.com

- Guía legal Ciberbullying y Grooming de Inteco, ahora INCIBE. http://www.educacion.navarra.es/portal/digitalAssets/49/49141_20110336.pdf
- Guía adolescencia y Sexting de Inteco, ahora INCIBE. https://www.incibe.es/CERT/guias_estudios/guias/Guia_sexting
- Estudio sobre fraude a través de Internet de INCIBE. https://www.incibe.es/CERT/guias_estudios/Estudio_fraude_1C2012
- Web dependiente del INCIBE, Instituto Nacional de Tecnologías de la Comunicación. www.osi.es/recursos/utiles-gratuitos
- Guía de actuación contra el Ciberacoso de Inteco, ahora INCIBE. http://www.chaval.es/chavales/sites/default/files/editor/guia_lucha_ciberacoso_menores_osi.pdf
- Ciberbullying, guía de recursos del Defensor del menor. http://www.educacion.navarra.es/portal/digitalAssets/49/49132_20010331.pdf
- → Ciberbullying: Prevenir y actuar de la Comunidad de Madrid. http://www.copmadrid.org/webcopm/recursos/CiberbullyingB.pdf
- Protocolo ante ciberbullying Gobierno Vasco. http://www.emici.net/prot/Protocolo%20Ciberbullying.html
- Estudio de Menores de Edad y Conectividad móvil en España de Protégeles.
 http://www.diainternetsegura.es/descargas/estudio_movil_smartphones_tablets_v2c.pdf
- Navegadores infantiles. www.kidoz.net
- Buscadores infantiles. www.buscadorinfantil.com www.kidrex.org
- Youtube Kids. https://www.youtube.com/channel/UC7Pq3Ko42YpkCB Q4E981jw
- Web dedicada a la privacidad de Save the Children. www.deaquinopasas.org
- Recomendaciones a usuarios de Internet de Agencia española de protección de datos. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/g uia_recomendaciones_internet_052009.pdf
- Guía Derechos de niños y niñas, deberes de padres y madres, destinada a los menores de Agencia española de protección de datos. www.agpd.es/portalwebAGPD/canal_joven/common/pdfs/recomendaciones_menores_ 2008.pdf
- Web de Gobierno de Navarra dedicada a Seguridad Informática y menores. http://www.disfrutalared.com/index.php/es/

Este es un documento elaborado por <u>Fundación Dédalo</u> y financiado por el <u>Departamento de Educación del Gobierno de Navarra</u> **Gobierno de Navarra** Departamento de Educación