Protección de la Infancia en Línea: Guía para padres, tutores y educadores

www.itu.int/cop

Notificación legal

El presente documento puede ser actualizado en cualquier momento.

Las fuentes externas se mencionan, en su caso. La Unión Internacional de Telecomunicaciones (UIT) no se hace responsable del contenido de las fuentes externas, incluidos los sitios web externos mencionados en la presente publicación.

Ni la UIT ni ninguno de sus representantes será responsable de la utilización de la información contenida en la presente publicación.

Descargo de responsabilidad

La mención de países, empresas, productos, iniciativas o directrices específicos, o las referencias a los mismos, no implican en modo alguno que las apoyen o recomienden la UIT, los autores o cualquier otra organización a la cual estén afiliados los autores antes que otras de carácter similar que no se mencionen.

Las solicitudes de reproducción de extractos de la presente publicación pueden enviarse a: jur@itu.int

© Unión Internacional de Telecomunicaciones (UIT), 2009

RECONOCIMIENTOS

Esta Guía ha sido preparada por la UIT y un equipo de autores de instituciones destacadas activas del sector de las TIC, y no habría sido posible sin su tiempo, entusiasmo y dedicación.

La UIT expresa su agradecimiento a todos los autores siguientes, que han aportado su tiempo y valiosos análisis: (por orden alfabético)

- Cristina Bueti y Sandra Pandi (UIT)
- John Carr (*Children's Charities' Coalition on Internet Safety*)
- Ethel Quayle (Universidad de Edimburgo, Reino Unido)
- Janice Richardson (*Insafe network*)
- Isabella Santa (*European Network and Information Security Agency*)
- Margareta Traung (*European Commission Safer Internet programme*)
- Nevine Tewfik (*The Suzanne Mubarak Women's International Peace Movement: CyberPeace Initiative*)

Los autores agradecen particularmente los estudios y comentarios detallados de John Carr del CHIS, Sonia Billard y Christiane Agbton-Johnson del UNIDIR y Katerina Christaki de ENISA.

La UIT da las gracias asimismo a Salma Abbasi de eWWG por su valiosa participación en la iniciativa Protección de la Infancia en Línea (PIeL).

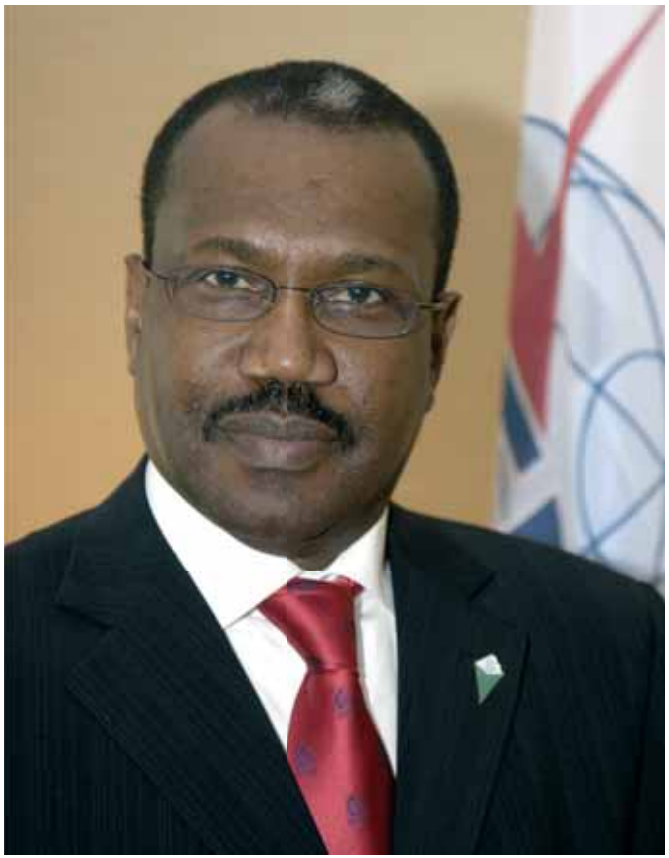
En la dirección www.itu.int/cop/ figura información y materiales adicionales sobre este proyecto de Guía, que se actualizará periódicamente.

Si tiene algún comentario o desea facilitar información adicional, diríjase a Cristina Bueti en la dirección cop@itu.int

Índice


“La Protección de la Infancia en Línea es un asunto mundial y por lo tanto, la respuesta debe ser mundial”

Prefacio



Ha llegado el momento de presentarles esta Guía preliminar elaborada con la valiosa ayuda de numerosos especialistas.

Con la generalización de Internet de banda ancha, la Protección de la Infancia en Línea es fundamental y exige una respuesta mundial coordinada. Las iniciativas locales e incluso nacionales son muy importantes, pero Internet no tiene fronteras y la cooperación internacional será fundamental para ganar la batalla que debemos librar.

Padres, tutores y educadores estarán en vanguardia de la lucha contra la ciberdelincuencia y la ciberamenazas, y les agradezco mucho su ayuda.

Dr. Hamadoun I. Touré
Secretario General de la Unión Internacional de Telecomunicaciones (UIT)

Exposición resumida

Internet ha aportado incontables beneficios a los niños de todo el mundo, y el número de hogares conectados aumenta cada año. A principios de 2009, había más de 1.500 millones de personas en línea, cuando apenas eran 200 millones a principios de 1998.

Ahora bien, aunque los posibles beneficios son indiscutibles, Internet no deja de ser motivo de preocupaciones, especialmente en lo que respecta a los niños.

Los conocimientos técnicos de los niños de hoy son sorprendentes. Son capaces de dominar rápida y fácilmente programas y aplicaciones muy complejos en ordenadores, aparatos móviles y otros dispositivos personales, y además parecen hacerlo casi instintivamente. En cambio, los adultos suelen necesitar un manual de instrucciones para comprender programas informáticos y aparatos móviles o personales que para los niños son como coser y cantar. Lo que sí pueden aportar en cambio los adultos al debate sobre la ciberseguridad son conocimientos y experiencia.

Lo importante es determinar lo que hacen realmente los niños y jóvenes en línea, y no lo que los adultos piensan que hacen. Se está demostrando que cada vez más niños se conectan a Internet a través de consolas de juegos y aparatos móviles, y muchos adultos no saben que es posible conectarse con esos aparatos.

Un parámetro importante es que niños y jóvenes tienden a conectarse a Internet en lugares que los adultos consideran seguros, es decir, el hogar y la escuela. Muchos padres y tutores tienen la idea equivocada de que sus niños están más seguros con un computador en casa que si accedieran a Internet en otro lugar. Es una idea peligrosa porque Internet puede llevar a niños y jóvenes prácticamente a cualquier lugar del mundo y exponerlos a peligros potenciales, exactamente como en el mundo real.

Esta Guía forma parte de la iniciativa Protección de la Infancia en Línea (PIeL)[1], que se enmarca en la Agenda sobre Ciberseguridad Global de la UIT[2], cuyo objetivo es definir las bases de un cibermundo física e intelectualmente seguro para todos los jóvenes de hoy y también para las generaciones futuras.

Esta Guía es un modelo que se puede adaptar y utilizar de modo que corresponda a las costumbres y legislaciones nacionales o locales.

[1] http://www.itu.int/cop

[2] http://www.itu.int/osg/csd/cybersecurity/gca/

Según la Convención de las Naciones Unidas sobre los Derechos del Niño, un niño es todo ser humano menor de 18 años de edad. La presente Guía trata de todo lo que puede afectar a las personas de menos de 18 años de edad en todas las regiones del mundo. Ahora bien, es muy improbable que un joven usuario de Internet de siete años de edad tenga los mismos intereses o necesidades que otro de 12 años que acaba de empezar la escuela secundaria, u otro de 17 que ya casi es adulto. Los consejos o recomendaciones que figuran en los distintos puntos de esta Guía corresponden a esos distintos contextos. Si bien las categorías generales pueden ser útiles nunca debemos olvidar que, al fin y al cabo, cada niño es diferente y sus necesidades específicas deben ser objeto de atención particular. Además, existen numerosos factores locales, legislativos y culturales que pueden influenciar notablemente la utilización o interpretación de esta Guía en los distintos países o regiones.

Existe ahora un acervo considerable de leyes e instrumentos internacionales que sustentan y, en muchos casos, exigen medidas para proteger a los niños en general, y también en particular con respecto a Internet. Esos instrumentos y leyes son la base de la presente Guía. Se resumen exhaustivamente en la Declaración y el Llamamiento de Río de Janeiro para impedir y detener la explotación sexual de niños y adolescentes, adoptada por el tercer Congreso Mundial contra la explotación sexual de niños y adolescentes en noviembre de 2008.

Además, puede observarse que en esta Guía se abordan cuestiones que pueden afectar a todos los niños y jóvenes menores de 18 años, aunque cada edad tiene sus propias necesidades. De hecho, cada niño es único y se merece una atención particular.

La UIT ha preparado esta Guía en estrecha colaboración con un equipo de autores de importantes instituciones activas en el sector de las TIC, a saber, el Programa de la UE para una Internet más Segura, el Organismo Europeo de Seguridad de las redes y la información (ENISA)[3], la Coalición Internacional para los niños en defensa de la seguridad en Internet, la iniciativa Ciberpaz y la Universidad de Edimburgo (Reino Unido). También se han recibido valiosísimas contribuciones de varios gobiernos nacionales y empresas de alta tecnología que comparten el objetivo común de lograr que Internet sea un lugar mejor y más seguro para niños y jóvenes.

La UIT, junto con los demás autores del presente Informe, pide a todos los interesados que promuevan la adopción de políticas y estrategias que protejan a los niños en el ciberespacio y promuevan un acceso seguro a los recursos en línea.

Esto permitirá crear una sociedad de la información más integradora y también ayudará a los Estados Miembros de la UIT a cumplir con sus obligaciones en la protección de los niños y la concretización de sus derechos, estipulados en la Convención de las Naciones Unidas sobre los Derechos del Niño[4] adoptada por la Asamblea General de las Naciones Unidas en su Resolución 44/25 de 20 de noviembre de 1989, y en los documentos producidos por la CMSI[5].

[3] http://www.enisa.europa.eu

[4] http://www.unicef.org/crc

[5] http://www.itu.int/wsis/outcome/booklet.pdf

Guía para padres, tutores y educadores

Esta sección tiene por objeto dar indicaciones a padres, tutores y educadores para que puedan ayudar a los niños a navegar por Internet de manera segura y positiva. En la página 49 figura una lista más completa de lo que se ha de tener en cuenta.

Padres, tutores y educadores		
	#	Lo que se ha de tener en cuenta
1. Seguridad y protección de su ordenador personal	a.	Colocar el computador en una sala común
	b.	Instalar cortafuegos y antivirus
2. Reglas	a.	Acordar reglas domésticas sobre la utilización de Internet y de aparatos personales, prestando particular atención a cuestiones de privacidad, edad, lugares inapropiados, acoso y al peligro que representan los extraños
	b.	Acordar reglas sobre la utilización de aparatos móviles
3. Información de padres, tutores y maestros	a.	Padres, tutores y maestros deben estar familiarizados con los sitios Internet que utilizan sus niños y deben tener una idea bastante precisa de lo que hacen los niños cuando están en línea
	b.	Padres, tutores y educadores deben saber cómo los niños utilizan otros aparatos personales tales como teléfonos móviles, consolas de juego, lectores MP3, PDA, etc.

4. Información de los niños	a.	Informe a sus niños sobre los riesgos que entraña la divulgación de información personal, la organización de encuentros físicos con personas conocidas en línea, la divulgación de fotografías en línea; la utilización de webcams, etc.
5. Comunicación	a.	Hable con sus niños de sus experiencias

1. Antecedentes

La Cumbre Mundial sobre la Sociedad de la Información (CMSI), que se celebró en dos fases en Ginebra (10-12 de diciembre de 2003) y Túnez (16-18 de noviembre de 2005), concluyó con el audaz compromiso de "construir una sociedad de la información centrada en la persona, integradora y orientada al desarrollo, en que todos puedan crear, consultar, utilizar y compartir la información y el conocimiento" (Declaración de Principios de Ginebra, punto 1).

En la CMSI, los líderes de la comunidad internacional encomendaron a la UIT la Línea de Acción C5: "Creación de confianza y seguridad en la utilización de las TIC".

En los resultados de la CMSI también se reconocen específicamente las necesidades de niños y jóvenes y su protección en el ciberespacio.

En el Compromiso de Túnez se reconoce "el papel de las tecnologías de la información y la comunicación (TIC) en la protección y en la mejora del progreso de los niños", así como la necesidad de "reforzar las medidas de protección de los niños contra cualquier tipo de abuso y las de defensa de sus derechos en el contexto de las TIC".

Solemos dar por sentado[6] que, por lo general, sabemos siempre dónde están nuestros niños, con quién están y lo que están haciendo.

Ahora bien, en el mundo digital, donde incluso los más jóvenes pasan cada vez más tiempo en línea, acabamos siendo meros espectado-

[6] http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online

“Los adultos aportan sus conocimientos y su experiencia al debate sobre la ciberseguridad”

res y muchos de nosotros estamos aquejados de una especie de "traumatismo digital".

Los niños, incluso los más jóvenes, conocen probablemente mejor la tecnología actual que sus educadores o padres.

Los niños de hoy sólo conocen un mundo lleno de electrónica, donde la tecnología está integrada en todos los aspectos de sus vidas.

Les sirve para cultivar amistades, aprender, y comprender el mundo y las personas que los rodean. Entretanto, los adultos tratamos de adivinar las reglas que conviene fijar y cómo aplicarlas.

El problema es que este tema en particular no se aborda en los libros para padres; ese capítulo todavía no se ha escrito y la sociedad no ha tenido tiempo de definir normas.

Existe una edad legal para beber alcohol y otra para conducir, pero nadie sabe a ciencia cierta a qué edad los niños pueden navegar solos con seguridad o enviar un mensaje de texto con el móvil, ni hasta qué punto los padres deben vigilar a sus niños, tan vulnerables y a menudo inocentes, durante sus actividades en línea.

Hay una diferencia desconcertante entre lo que creen los padres que saben sus niños, y lo que éstos saben en realidad.

Si bien 92% de los padres dicen que han definido reglas para las actividades en línea de sus hijos, 34% de los niños dicen que sus padres no lo hacen. Estas proporciones son casi las mismas en todos los países del mundo:

En Francia, 72% de los niños navegan solos en línea, y si bien 85% de los padres saben que existen programas de control parental, sólo 30% los instalan.

En Corea, 90% de los hogares están conectados a banda ancha de alta velocidad muy barata, y hasta 30% de los coreanos de menos de 18 años de edad corren peligro de convertirse en adictos de Internet y pasar dos horas o más en línea cada día.

En el Reino Unido, 57% de los niños de entre 9 y 19 años de edad dicen que han visto pornografía en línea, 46% dicen que han dado información que no debían, y 33% dicen que han sido acosados en línea.

En China, 44% de los niños dicen que extraños han tratado de entablar contacto con ellos en línea, y 41% han hablado de sexo o de algún tema que les resultaba incómodo con un extraño en línea.

Para afrontar estas crecientes dificultades, la UIT, junto con otros interesados, lanzó la iniciativa Protección de la Infancia en Línea (PIeL)[7] en noviembre de 2008.

La iniciativa PIeL de la UIT forma parte de su Agenda sobre Ciberseguridad Global (GCA)[8] y tiene por objeto ser una red de colaboración internacional para tomar medidas a fin de promover la protección de niños y jóvenes en línea en todo el mundo, dando indicaciones sobre comportamientos seguros en línea junto con otros organismos de las Naciones Unidas y asociados.

[7] www.itu.int/cop

[8] www.itu.int/osg/csd/gca

Los principales objetivos de la iniciativa PIeL son los siguientes:

- identificar los riesgos y vulnerabilidades de los niños y jóvenes en el ciberespacio;
- sensibilizar al público sobre todo lo relacionado con los riesgos de Internet, por todos los medios posibles;
- crear instrumentos prácticos para ayudar a gobiernos, organizaciones y educadores a minimizar los riesgos;
- compartir conocimientos y experiencias y facilitar las asociaciones estratégicas internacionales para definir y aplicar iniciativas concretas;
- esta Guía se ha preparado en el marco de la iniciativa Protección de la Infancia en Línea (PIeL) de la UIT y tiene por objeto facilitar información, consejos y trucos de seguridad a padres, tutores y educadores sobre la protección de los niños en línea.

2. Niños y jóvenes en línea

Internet ha cambiado mucho en los últimos años. Nuevos servicios como blogs, Wikipedia, MySpace, You Tube y juegos en línea, han aumentado las posibilidades de conexión a Internet, fomentado los contactos sociales y permitiendo que los navegantes creen su propio contenido. El número de nuevos blogs se ha duplicado cada cinco meses durante los dos últimos años y la utilización de sitios de contacto social tales como Bebo, Facebook, Habbo y Twitter se multiplica cada año. Además, durante los últimos tres años, la comunicación entre usuarios se ha convertido en el principal tráfico Internet.

Niños y jóvenes son usuarios activos y entusiastas de las TIC, que utilizan para charlar y compartir información personal y les ofrecen numerosas oportunidades positivas de participación, creatividad y educación. También permite que jóvenes de todas las nacionalidades, religiones y culturas puedan comunicar. En el cuadro siguiente, por ejemplo, se describen los tipos de experiencia en línea que tendrán más probablemente los niños cuando accedan a mundos virtuales[9]:

[9] ENISA, *Children on virtual worlds - What parents should know*, septiembre de 2008, en la dirección http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

Tipo de comportamiento	Sus intereses	Son probablemente...	Características
Exploración-investigación	En busca de algo, resolver un misterio, ir de viaje, estar "al aire libre"	Los niños más seguros de sí mismos, sin distinción de edad o sexo	Se fijan en los detalles, son curiosos y comunicativos, vuelcan su imaginación en el misterio
Autoafirmación	Presentarse al mundo	Ambos sexos, posiblemente niños más mayores	Niños y niñas quieren "dejar su huella" en su avatar, quizá con su propia cara; las niñas más mayores quieren vestir y maquillar sus avatares. Niños y niñas desean expresarse mediante la creación de un hogar o "base"
Ascensión social	Categoría, posición social en el entorno	Niños más jóvenes y mayores; ligera distinción entre los sexos (los niños ligeramente más que las niñas)	Competitivos; les preocupa su categoría y mostrar esa categoría a los demás
Peleas	Muerte y destrucción, violencia y superpoderes	Varones, ligera tendencia a ser niños más mayores	Los niños expresan sus frustraciones cuando no disponen de medios para expresarse; las posibilidades de "ganar" y "derrotar a los oponentes" limitan las frustraciones

Tipo de comportamiento	Sus intereses	Son probablemente...	Características
Colección-consumismo	Acumular todo lo que parezca tener valor en el sistema	Niños y niñas más mayores	Coleccionan páginas y créditos, buscan tiendas, oportunidades de hacer regalos, una economía y un lugar para poner sus pertenencias
Usuarios experimentados	Hacen beneficiar a todos de sus conocimientos y experiencias	Expertos en juegos, la geografía de los entornos, los sistemas	Dedican varias horas seguidas a jugar y explorar el juego, se interesan mucho por los entresijos del juego
Creadores de universos virtuales	Creación de nuevos universos, nuevos elementos en el universo, población del universo	Niños más jóvenes (mundos imaginarios sin reglas), y niños más mayores (mundos imaginarios con reglas y sistemas –casas, escuelas, tiendas, transporte, economía)	Los niños expresan su frustración cuando no disponen de medios para expresarse; los sistemas (o ausencia de los mismos) para regir el entorno son interesantes
Criadores	Se ocupan de sus avatares y mascotas	Niños y niñas más jóvenes, y niñas más mayores	Los niños quieren conocer a otros y jugar con ellos, enseñar a sus avatares trucos como nadar, y tener un lugar para que puedan dormir. Las mascotas virtuales también son interesantes

Internet es un medio completamente neutro de divulgación de datos que pueden servir para hacer el bien o el mal.

Por una parte, por ejemplo, es una magnífica fuente de conocimientos para personas de todas las edades y aptitudes.

Por otra parte, Internet se puede utilizar para poner trampas y explotar a los usuarios con fines delictivos y, lamentablemente, los niños son los que caen más fácilmente en ese tipo de trampas.

Es importante recordar que Internet no es el único medio de comunicación que puede perjudicar a los niños.

Durante los últimos años, los jóvenes utilizan cada vez más sus teléfonos móviles, y los niños los utilizan para acceder a Internet desde prácticamente cualquier lugar.

Esto aumenta el riesgo de que estén expuestos a peligros en línea sin la supervisión de un adulto.

En Corea, por ejemplo, la edad media de los niños que reciben su primer teléfono móvil es de unos ocho años.

Es importante recordar que los teléfonos móviles también han evolucionado recientemente.

Ahora se pueden utilizar para mensajería de vídeo, servicios de esparcimiento (telecarga de juegos, música y vídeo), así como para acceder a Internet y utilizar servicios basados en la localización.

Los riesgos que pueden correr los niños que acceden a Internet a través de teléfonos móviles u otros aparatos personales son similares a los de Internet con una conexión alámbrica.

La gran diferencia entre el acceso a Internet a través del teléfono móvil o de un ordenador portátil, en comparación con el acceso tradicional a través de un ordenador doméstico, es el carácter sumamente privado de esos aparatos personales móviles.

Cuando los adolescentes utilizan aparatos personales, los padres no suelen poder supervisarlos directamente como harían en un ordenador doméstico.

Los padres deben hablar con sus hijos de la utilización de esos aparatos y asegurarse de que pueden controlarlos cuando los adquieren o utilizan por primera vez.

Estudio práctico: Jóvenes egipcios e Internet

El grupo sobre la seguridad de los jóvenes egipcios en Internet (Net-Aman) consta de 11 miembros de 18 a 28 años de edad, y forma parte integrante de la iniciativa Ciberpaz ideada por el Movimiento Internacional de Mujeres para la Paz de Suzanne Mubarak con apoyo de varios asociados.

El nombre de este grupo es Net-Aman ("seguridad en la red" en árabe), y lo han elegido todos los jóvenes del grupo.

El mandato del grupo consiste en aumentar la sensibilización sobre la seguridad en Internet y las ingentes posibilidades de las TIC, con objeto de ofrecer a niños y jóvenes la posibilidad de identificar ellos mismos contenidos perjudiciales, decidir ellos mismos la manera ideal de abordarlos, y compartir experiencias.

La primera sesión de formación de Net-Aman elaboró un cuestionario que los miembros utilizaron para obtener una "instantánea" de las inquietudes y esperanzas de niños y jóvenes acerca de la utilización de Internet en Egipto.

Se encargó a los jóvenes que fueran a escuelas y universidades y sometieran un informe sobre las conclusiones de la encuesta a la segunda sesión de capacitación de marzo de 2008. La encuesta se efectuó entre varios jóvenes que representaban diversos grupos de edades de 8 a 22 años.

Esa encuesta ayudó a Net-Aman a comprender lo que piensan los jóvenes egipcios acerca de Internet y su seguridad.

Aproximadamente 800 jóvenes egipcios respondieron a la encuesta *youth2youth* titulada "Jóvenes egipcios e Internet".

Los niños y jóvenes encuestados afirmaron que:

- Ningún adulto los vigila cuando utilizan Internet.
- En lo que respecta a los riesgos y dificultades de Internet en Egipto, señalaron que el contenido inapropiado representa el principal riesgo en línea, a continuación los virus y programas espías, contenido violento, deberes copiados (plagio), y por último el ciberacoso.
- Uno de los resultados más chocantes de la encuesta fue que la mayoría de los jóvenes divulgan su información personal, nombre completo, edad, fotografías, información escolar y números telefónicos por Internet sin preocuparse en modo alguno de las consecuencias.

A la luz de los resultados de esta encuesta y de acuerdo con el mandato del grupo sobre la seguridad de los jóvenes egipcios en Internet (Net-Aman), los jóvenes seguirán aportando su contribución y participando en actividades que les ayudarán a aumentar la sensibilización de los jóvenes egipcios sobre las cuestiones de protección de los niños en línea.

Si desea información adicional, acuda al sitio web de Ciberpaz en la dirección: http://www.smwipm.cyberpeaceinitiative.org

3. Padres, tutores y educadores

Definición de padres, tutores y educadores

Varios sitios Internet se refieren a los padres de manera genérica (como en una "página de padres" y mencionan "controles parentales"). Por lo tanto, quizá sea útil definir las personas que, en un mundo ideal, deberían velar por que los niños utilicen sitios Internet de manera segura y responsable y dar su consentimiento para acceder a determinados sitios Internet.

En el presente documento "padres" significa madre y/o padre biológico de un niño, o persona a quien se ha encomendado su custodia.

En el mundo actual se dan muchos casos en que personas distintas de los padres biológicos se ocupan de los niños.

Suelen llamarse tutores o cuidadores, y es importante y fundamental reconocer su papel cuando los niños de los que se ocupan están en línea.

Un educador es una persona que trabaja sistemáticamente para mejorar los conocimientos de otra persona sobre un tema.

Educadores son personas que enseñan en las aulas y también otros que, de manera más informal, por ejemplo, trabajan en lugares de

contacto social para facilitar información sobre la seguridad en línea o imparten cursos comunitarios o escolares para que los niños estén seguros en línea.

El trabajo de los educadores depende del contexto en el cual trabajan y de la edad de los niños (o adultos) de los que se ocupan.

Todos los que están en contacto con niños y jóvenes –padres, maestros, asistentes sociales, bibliotecarios, animadores y miembros de la familia en general, como los abuelos. Es importante señalar que los niños que dependen de servicios sociales son particularmente vulnerables y, como tal, merecedores de una atención especial.

Por otra parte, es importante tener en cuenta la dinámica de grupo, porque es más fácil escuchar a los de su misma condición.

Lo que no saben muchos padres, tutores y educadores

En unos análisis recientes, ENISA ha observado que, en la mayoría de los casos, los padres y tutores desconocen detalles de las experiencias que sus niños pueden vivir en línea y los riesgos y vulnerabilidades que entrañan esas actividades.

Los niños pueden utilizar varios soportes y aparatos para conectarse en línea, tales como:

1. Ordenadores personales.
2. Teléfonos móviles.
3. Asistentes personales digitales (PDA).

Del tipo de plataforma utilizada y de sus características depende la experiencia de cada persona. Por ejemplo:

Característica	Descripción
Crear perfiles	Introducir información sobre uno mismo.
Interactividad con otros	Compartir información e ideas con otros usuarios en salas de charla, blogs, mensajería instantánea, foros de discusión y voz por protocolo Internet (VoIP).
Crear avatar	Elegir una imagen gráfica para representarse a uno mismo y afirmar su identidad en el sitio Internet.
Juegos	Demostrar sus capacidades intelectuales y ofrecer actividades para participar en línea.
Responder a cuestionarios	Concursos de entrenamiento cerebral, que suelen premiar la participación de alguna manera. Además, crea competencia entre amigos o grupos de amigos en forma de "cuadros de honor".
Dibujos, animaciones, tiras cómicas y artilugios	También llamado contenido generado por el usuario (UGC, *user generated content*), muchos niños disfrutan creando su propio contenido para compartirlo con su comunidad, y se desarrollan creativamente cuando colaboran con otros miembros de su comunidad virtual.
Creación de contenido, de música y danza a vídeo	Personas de todas las edades pueden publicar sus obras en línea, lo que puede ser una excelente válvula de escape creativa.
Compra de productos	Los usuarios pueden adquirir productos o servicios con dinero real.
Colgar fotografías o cualquier otra información	En algunos servicios los niños pueden subir fotografías e información. Algunos filtran contenido personal y/o otros contenidos inapropiados.
Telecargar música	Algunos servicios permiten que los niños telecarguen música.
Ver anuncios sobre productos/servicios	Los sitios Internet se financian a menudo con publicidad.

Los jóvenes se conectan en línea por diversos motivos, entre otros[10]:

1. Interactuar con amigos en un nuevo entorno, en tiempo real, compartiendo intereses comunes con otros.
2. Crear y adherirse a comunidades o grupos de interés, por ejemplo, música, fútbol, etc., comunicar ideas e información sobre temas de interés, mediante blogs, mensajería instantánea y otros.
3. Conocer nuevas personas e incluso hacer nuevos amigos.
4. Crear y compartir contenido original y personal, como imágenes, fotografías y vídeos, para aumentar las oportunidades de expresión personal.
5. Crear, publicar y compartir música.
6. Jugar.
7. Crear su propio espacio, aun cuando están presentes padres y cuidadores.
8. Experimentar con su identidad, nuevos espacios y fronteras sociales.

Aun cuando no es lo mismo acceder a un sitio Internet a través de un teléfono móvil o un PDA en lugar de un ordenador personal, los riesgos y vulnerabilidades asociados con la utilización de Internet son los mismos.

Una consideración esencial es que niños y jóvenes tienden a acceder a Internet en lugares donde les decimos que es seguro, es decir en el hogar y la escuela. Padres y tutores cometen los mismos errores y, a menudo, dicen que prefieren que sus niños estén en casa con un computador que en la calle, y no saber lo que hacen. Por supuesto, Internet puede llevar a niños y jóvenes a cualquier lugar y exponerlos a los mismos riesgos que en el mundo real. (Véase el recuadro en la página 21).

[10] Home Office, *Home office task force on child protection on the internet – Good practice guidelines for the providers of social networking and other user interactive services 2008*, 2008, available at http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary (last visited on 16 June 2008).

Estudio práctico: la privacidad en peligro

¡Muchos usuarios no son conscientes de la información personal que divulgan en línea, y hasta ni saben cómo lo han hecho!

- En muchos casos:
- Olvidan comprobar los parámetros de seguridad.
- Dan más información de la necesaria.

Cuando se trata de niños y jóvenes, esto los expone a contactos (quizá) inapropiados de otros niños, jóvenes más mayores o incluso adultos. Los niños también pueden dar inocentemente información sobre ellos mismos:

- Rellenando cualquier tipo de formulario (por ejemplo concurso e inscripción).
- Colgando perfiles personales.
- Creando un sitio web.

Es importante que los padres no exageren los riesgos o asusten a los niños indebidamente cuando les explican los riesgos a que se exponen en línea.

Saber cómo los niños pueden divulgar con total inocencia información en línea, y la facilidad con la que extraños pueden encontrar esa información, es una de las consideraciones importantes que se han de tener en cuenta.

Los niños deben saber que existen muchas bases de datos que pueden facilitar información sobre su dirección, número de teléfono y dirección de correo electrónico.

Se ha de alentar a niños y jóvenes a utilizar los parámetros de privacidad en todo momento cuando están en línea y avisar a un adulto responsable si se les pide información personal (física) o si la comunicación en línea les resulta incómoda.

A continuación, una charla ficticia que, según las autoridades, es muy común en línea. Imaginemos un pedófilo predador que toma notas sobre el niño y utiliza esa información para engañarlo. ¿Se dejaría engañar su hijo? Lamentablemente, algunos sí.

Niño: ¡Odio a mi madre! Sé que es culpa suya si mis padres se divorcian.

Predador: Ya sé. Mis padres también se están divorciando.

Niño: Nunca tenemos dinero. Siempre que necesito algo, dice lo mismo "No nos lo podemos permitir". Cuando mis padres estaban juntos, podía comprar cosas. Ahora no puedo.

Predador: Yo también ¡lo odio!

Niño: Llevo seis meses esperando que salga un nuevo juego informático. Mi mamá me prometió comprármelo cuando saliera. ¡Lo prometió! Ahora ha salido. ¿Lo puedo comprar? No. "¡No tenemos bastante dinero!". ¡Odio a mi madre!

Predador: ¡Oh! ¡Cuanto lo siento! ¡Ah, Ya sé! Tengo un tío muy simpático que siempre me compra cosas. Tiene mucho dinero.

Niño: Cuanta suerte tienes. Me gustaría tener un tío rico y simpático.

Predador: ¡Oye! ¡Tengo una idea! Le voy a preguntar a mi tío si te compraría uno también a ti... Como te he dicho es muy simpático. Seguro que dice que sí.

Niño: ¿De verdad? ¡¡Gracias!!

Predador: Espera un momento... Voy a preguntarle.

Predador: ¡Adivina! Ha dicho que sí. ¡Te va a comprar el juego!

Niño: Guau, ¿De verdad? gracias. ¡¡¡No me lo creo!!!

Predador: ¿Dónde vives?

Niño: Vivo en NJ. ¿Y tú?

Predador: Vivo en Nueva York. Mi tío también. Nueva Jersey no está lejos.

Niño: ¡Genial!

Predador: ¿Hay un centro comercial cerca de tu casa? Nos podemos ver allí.

Niño: De acuerdo. Vivo cerca del centro comercial GSP.

Predador: He oído hablar de él. Ningún problema. ¿Qué tal el sábado?

Niño: Genial.

Predador: Podemos ir también al McDonald's si quieres. Nos vemos allí a mediodía.

Niño: De acuerdo. ¿Dónde?

Predador: Frente a la tienda de informática. ¡Ah! Mi tío se llama George. Es realmente simpático.

Niño: Genial... gracias, te lo agradezco mucho. Qué suerte tienes de tener un tío rico y simpático.

Llega el sábado, y el niño va al centro comercial y se encuentra con un adulto fuera de la tienda de informática. Éste se identifica como "tío George" y explica que su sobrino ya está en el McDonald's esperándolos.

El niño se siente incómodo, pero el tío entra en la tienda y compra el juego de 100 USD. Sale de la tienda y se lo da al niño, que inmediatamente está encantado y baja las defensas.

En estos casos, las advertencias contra los peligros de los extraños no sirven. No es un extraño, es "tío Jorge", y prueba de ello es el juego informático. Se sube al coche del tío Jorge sin dudarlo para ver a su amigo en el McDonald's. El resto sale en el noticiario de la noche.

Es repugnante. Te revuelve el estómago, pero ocurre, no muy a menudo, pero lo suficiente para que haya que decirlo. (Cada año se detiene a varios centenares de ciberpredadores.) Una vez ya es demasiado, sobre todo si es su hijo. Saber cómo trabajan y los trucos que utilizan le ayudarán a enseñar a su hijo cómo evitar ser una víctima.

Origen: http://www.wiredkids.org/parents/parry_guide.html

Utilización de Internet: riesgos y vulnerabilidades en línea

Estar expuesto a contenido ilegal y perjudicial, como pornografía, juegos y otro contenido inapropiado para niños, y contactos con otros usuarios. En la mayoría de los casos, los operadores de esos sitios no toman medidas para limitar el acceso de los niños a la web.

Creación, recepción y divulgación de contenido ilegal y perjudicial.

Fingir ser otro, a menudo otro niño, con la intención deliberada de dañar, acosar o intimidar.

Contacto indeseable, especialmente con un adulto que se hace pasar por un niño.

Divulgación de información personal que puede entrañar riesgos de daño físico.

Intentos delictivos de hacerse pasar por otros usuarios de Internet, principalmente para obtener ganancias financieras. En algunos casos puede tratarse de robo de identidad, aunque suele tratarse entonces de fraudes contra adultos.

Daño físico en encuentros en la vida real con conocidos en línea, con el consiguiente riesgo de abuso físico y sexual.

Correos indeseados y anuncios de empresas que utilizan sitios Internet para promover productos destinados a públicos de diversas edades y/o centros de interés.

Utilización excesiva en detrimento de actividades sociales y/o al aire libre importantes para la salud, la creación de confianza, el desarrollo social y el bienestar en general.

Intimidación y acoso.

Automutilaciones, comportamientos destructores y violentos como la "violencia lúdica" (*happy slapping*).

Utilización compulsiva o excesiva de Internet o de los juegos en línea.

Contacto con el racismo y otro tipo de discursos e imágenes discriminatorios.

Difamación y daños a la reputación.

Violación de los derechos propios o ajenos mediante plagio y telecarga de contenido (especialmente fotos) sin permiso. Se ha demostrado que la apropiación y telecarga indebidas de fotografías sin permiso es perjudicial para los demás.

Violación de los derechos de autor de otras personas, por ejemplo, telecargando música, películas o programas de TV por los que se debería pagar.

Confiar en información imprecisa o incompleta encontrada en línea, o información de una fuente desconocida o poco fiable, o utilización de la misma.

Utilización no autorizada de tarjetas de crédito, las de los padres o de otras personas, para pagar cuotas de admisión u otros servicios y bienes.

Interpretación equivocada de la edad de una persona: un niño que pretende ser mayor para acceder a lugares inapropiados para su edad, o persona mayor que lo hace por los mismos motivos.

Utilización de la cuenta de correo electrónico de los padres sin su consentimiento: cuando es necesario el acuerdo parental para activar una cuenta en sitios virtuales para niños, los niños pueden acceder abusivamente a las cuentas de sus padres. Los padres pueden tener dificultades para suprimir ciertas cuentas de servicios cuando han sido activadas.

Publicidad indeseada: para vender sus productos algunas empresas envían correo basura a niños a través de sitios de mundos virtuales. Se plantea la cuestión del consentimiento del usuario y cómo debe obtenerse. La legislación al respecto es insuficiente y es obviamente muy difícil determinar a partir de qué edad un niño es capaz de comprender transacciones de datos. De hecho, la aplicación de esas reglas en Internet ya es motivo de gran inquietud y el acceso por teléfonos móviles agudiza el problema.

Concretamente, se indican a continuación las mayores inquietudes de los educadores que, a menudo, están insuficientemente preparados para afrontarlas:

Redes sociales – la manera en que jóvenes y niños viven su vida utilizando espacios sociales es muy diferente de lo que han conocido muchos educadores. La mayoría no comprende por qué es tan importante tener tantos "amigos" en la lista de contactos, pero el número de amigos se equipara a menudo a la popularidad de los usuarios.

Sexting (envío de contenidos eróticos) – fenómeno relativamente nuevo, en el cual niños y jóvenes corren riesgos personales colgando imágenes sexualmente provocativas de ellos mismos o enviándolas a amigos por teléfono móvil.

La manera en que los niños utilizan los nuevos medios –y no como pensamos que lo hacen– existe una buena documentación sobre investigaciones (en varios países) que pueden ayudar a apoyar este trabajo. (Véanse también en *EU Kids Online* resúmenes de problemas, riesgos etc., en la UE, en la dirección www.eukidsonline.net).

¿Dónde buscar ayuda? Muchos países tienen servicios de ayuda telefónica a los cuales niños y jóvenes pueden comunicar sus problemas. Son objeto de mucha publicidad, y la comunicación es diferente según los países. Es importante que niños y jóvenes sepan que nunca es demasiado tarde para señalar un problema y que, al hacerlo, pueden ayudar a otros.

Cómo los educadores pueden ser víctima de intimidaciones (por ejemplo, niños y jóvenes que crean sitios de amenazas sobre maestros y otros profesionales). Los educadores deben confiar en que pueden utilizar la tecnología con seguridad. Muchos educadores se sienten indefensos ante algunos de estos problemas y no saben exactamente cómo lograr que se suprima cierto material de los sitios, etc. El sitio web *teachtoday* contiene varias indicaciones muy interesantes sobre este tema y otros temas conexos. www.teachtoday.eu

Es importante insistir (como ya se ha dicho) en que, si bien algunos educadores no tienen tantos conocimientos tecnológicos como los niños y jóvenes, tienen en cambio mucha experiencia y conocimientos para ofrecer consejos, orientaciones y ayuda. Se ha de insistir sobre este particular en los cursos de capacitación de educadores sobre cuestiones de ciberseguridad.

En su estudio[11], el OPTEM señala sin embargo que los riesgos identificados por los propios niños parecen estar más relacionados con Internet que con los teléfonos móviles y son, entre otros:

Riesgos para el ordenador (como virus y pirateo).

Aparición indeseada de imágenes, o acceso equivocado a sitios web indeseados que muestran violencia o pornografía. (Los niños más mayores tienden a restar importancia a las consecuencias de una exposición accidental.)

Engaños y fraudes.

Ataques de tipo sexual por adultos malintencionados.

Aunque los niños reconocen que a veces se permiten comportamientos arriesgados, no parecen preocuparles mucho los riesgos inherentes de este tipo de comportamiento y prefieren tratar de resolver los problemas por sí mismos o con sus amigos. Puede deducirse, pues, que sólo se dirigen a sus padres u otros adultos cuando el problema

[11] http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/qualitative_study_2008/summary_report_en.pdf

puede ser "grave". Esto se da más a menudo con niños más mayores que podrían utilizar más fácilmente un botón de alarma[12] (como el desarrollado por la *Virtual Global Task Force*), aunque no es el caso de todos los niños. Podemos observar que los niños conscientes de los riesgos "disciplinan" sus propias actividades, pero a menudo no consideran que, cuando se trata de nuevas tecnologías, los adultos deben ser el punto de referencia para juzgar y supervisar el comportamiento de los jóvenes[13]. Debemos ser prudentes cuando distinguimos simplemente entre los mundos en línea y fuera de línea, ya que no corresponde a nuestras vidas cotidianas que están cada vez más asociadas con las tecnologías en línea. Para muchos niños significa tener que navegar cuidadosamente entre las oportunidades que les ofrece la tecnología (como explorar su identidad, crear amistades y aumentar su sociabilidad) y los riesgos (en lo que respecta a la privacidad, los malentendidos y las prácticas abusivas) que entraña la comunicación por Internet[14].

¿Desempeñamos todos el mismo papel?

Es importante recordar que, para niños y jóvenes, las principales fuentes de enseñanza son los maestros y los padres[15].

Según el UK Byron Report[16], las políticas de protección de los niños deberían comprender una campaña de sensibilización que fomente la formación de adultos (padres, maestros y tutores) que podrían no estar familiarizados con la tecnología, y dar autonomía a los niños animándolos a arriesgarse menos y tener en cuenta las consideraciones de seguridad.

El mensaje adecuado para la persona apropiada

El principal objetivo de ese tipo de campaña sería cambiar el comportamiento y, en particular, alentar comportamientos en línea más seguros de los niños, animar a los padres a vigilar más atentamente a los niños en línea y animar a las demás personas que están en contacto con niños (miembros de la familia en general, maestros, etc.) a enseñar a los niños a adoptar un comportamiento seguro en línea.

No debe considerarse que la seguridad de los niños en Internet es un asunto aislado, sino más bien que tiene puntos comunes con varias iniciativas sobre los niños, su seguridad e Internet.

12 http://www.virtualglobaltaskforce.com/

13 Quayle, E., Lööf, L. & Palmer, T. (2008), *Child Pornography and Sexual Exploitation Of Children Online*. Bangkok: ECPAT International.

14 Livingstone, S. *Taking risky opportunities in youthful content creation: teenager's use of social networking sites for intimacy, privacy and self-expression*. New Media and Society, 10 (3), 2008, 393-411.

15 Livingstone, S., Bober, M. *UK Children Go Online, Final report of key project findings*, April 2005

16 Byron, T. (2008) *Safer Children in a Digital World*.

Papel que pueden desempeñar los padres y tutores

Comportamiento que pueden adoptar los padres y tutores para asegurarse de que los niños utilizan Internet de manera segura y responsable:

1. Hablar a los niños de lo que hacen y con quien comunican cuando utilizan su ordenador o aparato personal, como un teléfono móvil o consola de juego. Entablar y mantener este diálogo es fundamental para ayudar a los niños a estar seguros.
2. Leer las condiciones de utilización con los niños antes de que entren en el sitio, hablar de las precauciones de seguridad, definir ciertas reglas básicas y supervisar la utilización para asegurarse de que se respetan las reglas.
3. Informar a los jóvenes usuarios sobre la utilización responsable de la tecnología en general, invitándolos a seguir su instinto y tener sentido común.
4. Comprobar si el sitio tiene soluciones técnicas tales como:
   - Filtros y controles parentales.
   - Registro del historial de usuario.
   - Moderación y, si así es, comprobar si son seres humanos o dispositivos automáticos que, por ejemplo, utilizan filtrado de texto que reconoce palabras y URL específicos. ¿Se recurre en el sitio a la intervención humana junto con sistemas técnicos? Los moderadores humanos están formados para garantizar un entorno seguro y apropiado. Suele decirse que los moderadores activos son personajes o participantes del mundo virtual o, en el contexto de los juegos, pueden hacerse pasar por invitados del juego y, en cualquier caso, siempre son visibles para todos los usuarios. Habitualmente, el moderador de un juego sólo interviene cuando se plantean situaciones difíciles pero, en algunos casos, ayudan a los usuarios que parecen "perdidos" o que necesitan ayuda. Los moderadores silenciosos suelen permanecer en un segundo plano y bloquean material ofensivo, reaccionan ante comportamientos sospechosos, previenen a los usuarios y llevan a cabo otras actividades disciplinarias.
   - Si el sitio permite colgar fotografías o vídeos, ¿los modera activamente o sólo examina las imágenes cuando recibe un informe?
   - Funcionalidades de información y bloqueo: suele disponerse de herramientas para comunicar contenidos, conversaciones y actividades inapropiados, tales como "banderas" y "botones de informe". El mundo virtual también debe indicar una política clara sobre cómo y a quién informar acerca de comportamientos inapropiados. Debería enseñarse a los niños a señalar incidentes o contactos indeseados y cómo bloquear esos contactos, utilizar opciones de privacidad y registrar conversaciones en línea.
   - Índices de evaluación: los padres y tutores deben conocer los símbolos de evaluación y su utilización, ya que son muy importantes para proteger a los jóvenes usuarios contra servicios y contenidos inapropiados.
   - Comprobación de la edad: si un sitio pretende verificar la edad, ¿cuál es la fiabilidad de su sistema? Si están en venta productos destinados a ciertas categorías de edad, ¿utilizan un sistema fiable para comprobar la edad?

5. Estar pendiente de las actividades de los jóvenes usuarios en línea. Es fundamental subrayar la importancia del papel que padres y cuidadores pueden y deben desempeñar en Internet, porque su participación influencia notablemente la opinión de los niños y promueve un comportamiento positivo.
6. Guardar la calma y no sacar conclusiones precipitadas si se escucha o ve algo preocupante acerca del comportamiento del niño o de uno de sus amigos en línea. Algunos sitios Internet son el único medio de contacto social de ciertos jóvenes. Si el niño teme que se le corte sencillamente ese vínculo social, es probable que sea cada vez más reacio a compartir los problemas o inquietudes que pueda tener.
7. Tenga en cuenta que el niño puede comportarse de manera muy diferente en línea y en la vida real, cara a cara con usted. No es inhabitual ser más agresivo en línea, donde se piensa que nadie pedirá cuentas. Aproveche los informes de comportamiento inapropiado que pueda recibir el niño para hablar con él del tono apropiado que conviene adoptar en las comunicaciones en línea.
8. Aprenda la cultura en línea para poder evaluar la autenticidad de las excusas habituales cuando se les reprocha su comportamiento en línea, tales como "alguien robó mi cuenta". Se dan muy pocos casos cuando se trata de mensajes y salas de charla que han violado las reglas de un mundo virtual. Puede ocurrir, pero es excepcional.
9. Explique al niño que no debe comunicar sus contraseñas de acceso a amigos o familiares. Éste es uno de los mayores problemas que plantean los sitios Internet a los jóvenes. Por ejemplo, el mejor amigo de un hermano puede robar bienes virtuales que el niño ha obtenido trabajosamente.
10. Utilice la página de contacto del sitio web para compartir sus inquietudes y preguntas. Es su responsabilidad asegurarse que usted se sienta cómodo con el sitio.
11. No se imagine que el niño es blanco de todo el mundo en Internet. Las estadísticas demuestran que los problemas con pedófilos en la vida real son mucho más numerosos que los incidentes en línea. Por lo general, los sitios para niños son seguros y pueden ofrecer una maravillosa experiencia creativa, social y educativa a su niño, pero sólo si usted se mantiene al corriente y participa.

Función que pueden desempeñar los educadores

Es muy importante que los educadores no den por supuesto lo que pueden saber o ignorar los niños y jóvenes sobre cuestiones de ciberseguridad. Existen muchos errores comunes sobre Internet y lo que es apropiado o no. Por ejemplo, muchos adolescentes se comunican sus contraseñas y lo consideran a menudo como una prueba de auténtica amistad.

Una misión importante de los educadores es informar a niños y jóvenes de la importancia de las contraseñas, cómo guardarlas a buen recaudo y crear una contraseña segura.

Asimismo, en lo que respecta a las cuestiones de derechos de autor, muchos adultos están horrorizados por la aparente indiferencia con que los jóvenes usuarios telecargan ilegalmente música y vídeos. Según diversas investigaciones[17] más que

[17] Berkman Center –*John Palfrey and Urs Gasser* — 2008

no preocuparse sobre los derechos de autor, niños y jóvenes carecen totalmente de conocimientos sobre la legalidad y los derechos de autor del contenido en línea. En este caso también, es evidente que los educadores tienen la importante misión de explicárselo a los alumnos.

Las escuelas tienen la oportunidad de transformar la enseñanza y ayudar a los alumnos a alcanzar su pleno potencial y a aumentar sus exigencias con respecto a las TIC. Ahora bien, también es importante que los niños aprendan un comportamiento seguro cuando utilizan estas nuevas tecnologías y en particular las de tipo Web 2.0 tales como los sitios de contacto social, que se están convirtiendo en un aspecto esencial de un aprendizaje social productivo y creativo. Los educadores pueden ayudar a los niños a utilizar la tecnología de manera sensata y segura de la manera siguiente[18]:

1. Asegurarse de que la escuela ha definido políticas y prácticas seguras y que su eficacia se controla y evalúa periódicamente.
2. Asegurarse de que todos conocen la política de utilización aceptable y su empleo. Es importante que esa política esté adaptada a las distintas edades.
3. Comprobar que la política de la escuela contra la intimidación hace referencia a la intimidación por Internet y teléfonos móviles u otros aparatos, y que existen sanciones eficaces para los que no respecten esa política.
4. Nombrar un coordinador de ciberseguridad.
5. Asegurarse de que la red de la escuela es segura y está protegida.
6. Recurrir exclusivamente a un proveedor de servicio Internet acreditado.
7. ¿Utilizar un producto de filtrado/supervisión?
8. Dar a todos los niños clase de ciberseguridad y precisar dónde, cómo y cuándo se impartirán.
9. Asegurarse de que todo el personal (incluido el personal de apoyo) ha recibido la formación adecuada y que pone periódicamente al día sus conocimientos.
10. Tener un solo punto de contacto en la escuela y poder recopilar y registrar los incidentes de ciberseguridad, que darán a la escuela un mejor conocimiento de las cuestiones o tendencias que se han de tener en cuenta.
11. Asegurarse de que el equipo de gestión y los directores de la escuela están suficientemente sensibilizados con respecto a la cuestión de la ciberseguridad.
12. Organizar una auditoría periódica de todas las medidas de ciberseguridad.

Consecuencias educativas y sicológicas

En los últimos años la utilización de Internet por los niños ha aumentado espectacularmente y ha entrañado inquietudes crecientes acerca de la seguridad en línea. Desde siempre se ha observado un miedo recurrente de los posibles peligros de las tecnologías de comunicación, en particular en lo que concierne a las jóvenes. No obstante, se ha aducido que cuando se han investigado realmente esos peligros se ha observado que en muchos casos la culpable no es la tecnología como tal, sino más bien cómo los propios niños utilizan la tecnología y las inquietudes sobre la pérdida del control parental[19]. Se ha considerado que los educadores desempeñan un papel esencial en la promoción y

[18] BECTA. *Safeguarding Children Online*. 2009.

[19] Cassell, J. & Cramer. M. *High Tech or High Risk: Moral Panics about Girls Online*. In T. McPherson (Ed.) *Digital Youth, Innovation, and the Unexpected*. The John D. and Catherine T.MacArthur Foundation Series on Digital Media and Learning. Cambridge, MA: The MIT Press, 2008. 53–76.

aplicación de la seguridad en Internet. Parece que los padres de todo el mundo consideran que las escuelas deberían desempeñar el papel protagonista en la educación de los niños sobre una utilización segura de la tecnología, y la *Children's Charities Coalition* también sugirió que "deberían darse indicaciones más claras a las escuelas sobre la utilización segura de Internet, el correo electrónico, las salas de charla, los sitios web de escuelas y los programas de filtrado y bloqueo" [20].

Al principio, la seguridad en línea consistía principalmente en soluciones tecnológicas, tales como programas de filtrado, pero últimamente se ha observado una mayor movilidad de la tecnología de la información y, por consiguiente, los ordenadores de sobremesa ya no son el único medio de acceder a Internet. En la actualidad, un número creciente de teléfonos móviles y consolas de juegos ofrecen conexiones de banda ancha y los niños pueden acceder a Internet desde la escuela, el hogar, la biblioteca, un café Internet, un restaurante de comida rápida, el club de jóvenes o incluso en los transportes públicos. Las escuelas ofrecen la oportunidad de trabajar en Internet, colectivamente en una red cerrada o sencillamente rodeado de otros niños. Las medidas obvias consisten, entre otras, en establecer medidas de seguridad eficaces en la red, pero debemos ir más allá. Los niños pueden tener aparatos personales que no están cubiertos por la protección de la red, y BECTA ha declarado que debería insistirse en lograr que todos comprendan los riesgos y actúen en consecuencia. Según ellos, esto significa concebir y aplicar políticas de ciberseguridad que exijan la participación de un gran número de grupos de interés tales como:

1. Directrices de escuela.
2. Miembros de consejos escolares.
3. Altos administradores.
4. Maestros.
5. Personal de apoyo.
6. Jóvenes y padres o cuidadores.
7. Personal de las autoridades locales.
8. Proveedores de servicios Internet (PSI), proveedores de otros servicios electrónicos (PSE), tales como creadores de sitios de contactos sociales, y consorcios de banda ancha regionales que colaboran estrechamente con los PSI y PSE sobre medidas de seguridad de las redes.

BECTA ha declarado que, habida cuenta de que todos esos grupos tienen conocimientos que pueden ayudar a determinar las políticas escolares, es importante consultarlos a todos. Ahora bien, definir estas políticas no basta y todos los que están en contacto con los niños deben adoptar métodos que ayuden a los jóvenes y al personal a identificar y adoptar un comportamiento seguro. Si todos estos grupos participan desde el principio, todos serán conscientes de la importancia de esas políticas y de su responsabilidad personal de concretizarlas. Crear un entorno TIC seguro para el aprendizaje comprende varios elementos importantes tales como:

1. una infraestructura de sensibilización global;
2. responsabilidades, políticas y procedimientos;
3. un surtido eficaz de herramientas tecnológicas;
4. una enseñanza completa en ciberseguridad;
5. un programa para todos los integrantes del establecimiento;
6. un proceso de supervisión que verifique constantemente la eficacia de lo anterior [21].

Todo ello debería estar incorporado en las políticas existentes de

[20] Children_s Charities_ Coalition for Internet Safety (2001). *_Working to make the Internet a safer place for kids_*. Available at www.communicationswhitepaper.gov.uk/pdf/responses/ccc_internet_safety.PDF

[21] BECTA. *Safeguarding Children Online: A Guide for School Leaders: 2009*. Available from www.becta.org.uk/schools/safety

seguridad de los niños en la escuela, en lugar de considerar que lo debe administrar únicamente un equipo TIC. No tiene mucho sentido pensar que la intimidación por Internet o teléfono móvil es distinta de la intimidación en la vida real. Tampoco significa que la tecnología no puede ser también una parte importante de la solución, de la manera siguiente:

1. Prevención y protección contra virus.
2. Sistemas de supervisión para controlar quién ha telecargado qué, cuándo se telecargó y qué ordenador se utilizó.
3. Filtrado y control de contenido para reducir al mínimo el contenido inapropiado en la red escolar.

Es evidente que los problemas que plantean las nuevas tecnologías no afectan a todos los niños y, cuando realmente se plantean problemas, dependen de la edad de los niños que utilizan esas tecnologías. A finales de 2008, la *US Internet Safety Technical Taskforce* publicó su Informe "Enhancing Child Safety & Online Technologies" que contenía información muy útil sobre investigaciones originales publicadas que tratan de solicitaciones sexuales, acoso e intimidación en línea y exposición a contenidos problemáticos[22]. En ese Informe se señaló que "es inquietante que los medios de información generales amplifiquen esos temores y los vuelvan desproporcionados con respecto a los riesgos que deben afrontar los jóvenes.

El peligro es que dejen de verse los riesgos y se limiten las probabilidades de que la sociedad estudie los factores que generan riesgos conocidos y, a menudo por inadvertencia, perjudican a los jóvenes de manera inesperada. Las noticias periodísticas sobre los delitos cometidos contra los niños a través de Internet parecen reflejar las opiniones polarizadas de profesionales y académicos que trabajan en este sector, que va de los que consideran que es peligroso distorsionar la amenaza que representa para los niños, y los que opinan que se ha subestimado mucho esta amenaza.

[22] ISTTF (2008). *Enhancing Child Safety and Online Technologies: Final Report of the Internet Safety Technical Task Force To the Multi-State Working Group on Social Networking of State Attorneys General of the United States.* Harvard University: The Berkman Center for Internet and Society.

Ahora bien, se considera preocupante que la tecnología utilizada en Internet pueda volver vulnerables a ciertos niños y que los educadores, junto con padres y tutores, tengan responsabilidades al respecto. Sabemos sorprendentemente poco sobre cómo los niños acaban siendo víctimas y los factores que aumentan su capacidad de resistencia. Los tratos injustos son, entre otros:

1. Solicitar o engatusar al niño.
2. Exponerlo a materiales problemáticos o ilegales.
3. Exponer a los jóvenes a un medio que pueda fomentar un comportamiento dañino.
4. Ciberintimidación.

En el cuadro siguiente pueden verse distintos tipos de riesgo[23]:

	Comercial	Agresivo	Sexual	Valores
Contenido (el niño es el destinatario)	Anuncios Correo indeseado Patrocinio Información personal	Contenido violento/ odioso	Contenido pornográfico o sexual indeseado	Información o consejos tendenciosos, racistas o engañosos
Contacto (el niño es un participante)	Busca/cosecha información personal	Intimidación, acoso u ofensa	Encontrarse con extraños, o ser engatusado	Daños autoinfligidos o persuasiones inoportunas
Conducta (el niño es un actor)	Telecargas ilegales, pirateo, juegos, engaños financieros o terrorismo	Intimidación o acoso de otra persona	Creación y telecarga de material inapropiado	Divulgación de información/ consejos engañosos

[23] Cuadro elaborado por el proyecto *EUKids Online* y mencionado en el punto 1.3 de Byron Review.

Solicitaciones o engatusamiento en línea

En el contexto de las solicitaciones sexuales, o engatusamiento, comprendemos más fácilmente el proceso de victimización, parcialmente porque los propios niños han participado en gran medida en la investigación.

Una parte considerable de esta investigación procede del *Crimes against Children Research Center* (CCRC) de la Universidad de New Hampshire, y se fundamenta en dos estudios (YISS-1 e YISS-2), que consistió en encuestas telefónicas con muestras nacionales de usuarios de Internet de 10 a 17 años de edad, realizadas en 2000 y 2005[24]. Esta cuestión también se menciona en la International *Youth Advisory Council Global Online Survey* [25, 26].

Esos investigadores han declarado recientemente que sus trabajos sobre los delitos sexuales iniciados en Internet dejan claro que el estereotipo del agresor de niños en Internet que recurre a trucos y violencia para agredir a los niños es en gran parte impreciso[27].

Según estas investigaciones realizadas en Estados Unidos, en la mayoría de los delitos sexuales iniciados en Internet se trata de hombres adultos que utilizan ese medio para conocer y seducir a adolescentes menores a fin de obtener relaciones sexuales.

Los delincuentes utilizan comunicaciones Internet tales como mensajes instantáneos, correo electrónico y salas de charlas para conocer y desarrollar relaciones íntimas con sus víctimas.

Estos trabajos indican que en la gran mayoría de los casos, las víctimas saben que están conversando en línea con adultos.

Hasta la fecha, se han estudiado sobre todo los problemas de los niños que son víctimas de prácticas abusivas y se han ignorado los tipos de mundos sociales y culturales que los jóvenes crean en línea.

Ahora bien, los niños y adolescentes no son simples blancos de creaciones de adultos en Internet, también contribuyen activamente a la creación de sus propias ciberculturas.

En los estudios de la Universidad de New Hampshire se insiste en que son esos aspectos de Internet los que generan riesgos para algunos jóvenes que adoptan comportamientos específicos con las nuevas tecnologías.

Aunque la mayoría de los jóvenes parece *arriesgarse* (y en particular niños varones más mayores), la gran mayoría de los niños no parece *correr riesgos* [28].

Con todo, es más probable que los jóvenes que envían información personal (por ejemplo, nombre, número de teléfono, fotografías) a extraños, o hablan de sexo en línea con ese tipo de personas, reciban solicitaciones sexuales agresivas con intentos de contacto, o contactos reales en la vida real.

Durante los cinco años transcurridos entre YISS-1 y 2 se observó una disminución global de las solicitaciones sexuales, aunque esa tendencia no se observó entre jóvenes minoritarios y los que viven en hogares menos acomodados.

Los autores consideran que este aumento del acoso se debe en gran medida al aumento de la utilización de Internet durante los cinco años anteriores.

Ahora bien, en 2005 había 1,7 veces más probabilidades de que jóvenes señalaran solicitaciones agresivas, aun si se tienen en cuenta

---

[24] Finkelhor, D., Mitchell, K. and Wolak, J. *Online victimization: A report on the nation's youth.* (NCMEC 6-00-020). Alexandria, VA: National Center for Missing and Exploited Children. 2000.

[25] Wolak, J. Mitchell, K. and Finkelhor, D. *Online victimization: 5 year later* (NCMEC 07-06-025). Alexandria, VA: National Center for Missing and Exploited Children. 2006.

[26] http://www.virtualglobaltaskforce.com/iyac_charter_supp.pdf

[27] Wolak, J., Finkelhor, D., Mitchell, K.J., and Ybarra, M.L. *Online "predators" and their victims.* American Psychologist, 63 (2), 2008, 111-128.

[28] OPTEM. *Safer Internet for Children. Qualitative Study in 29 European Centres.* Brussels: European Commission. 2007.

los cambios demográficos y de la utilización de Internet y sus características.

Los factores de riesgo identificados para ese tipo de solicitaciones agresivas son, entre otros, el ser mujer, utilizar salas de charla, utilizar Internet móvil, hablar con personas conocidas en Internet, enviar información personal a personas que se ha conocido en línea, y sufrir abusos físicos o sexuales en el mundo real.

En la segunda encuesta, 4% (65 casos) señalaron una solicitud en línea de enviar una fotografía sexual de sí mismos durante el año anterior, pero sólo un joven lo hizo realmente.

Ser mujer, de origen afroamericano, tener una estrecha relación en línea, tener comportamientos sexuales en línea y ser víctima de abusos sexuales o físicos en el mundo real eran factores de riesgo para recibir una solicitud de fotografía sexual.

Es interesante observar que los jóvenes tienen más probabilidades de recibir solicitudes cuando están con amigos y comunican con un adulto, alguien que han conocido en línea, que ha enviado una fotografía sexual al joven y que ha tratado o conseguido entablar algún tipo de contacto en el mundo real[29].

En la primera encuesta parece que las solicitaciones sexuales están asociadas con síntomas de depresión[30].

Los jóvenes que señalaron importantes síntomas de tipo depresivo tenían 3,5 veces más probabilidades de señalar una solicitación sexual en línea no deseada en comparación con los que presentaban síntomas leves o ningún síntoma, y los que presentaban esos síntomas tenían dos veces más probabilidades de sentirse emocionalmente perturbados por el incidente.

Por lo general, la angustia era más común entre niños más jóvenes, aquellos que recibieron solicitaciones agresivas y los que recibieron solicitaciones en un ordenador fuera de casa[31].

En un estudio reciente en Suecia se estudiaron los niños de 16 años de edad que habían recibido solicitudes de encuentros sexuales en línea y en la vida real.

Entre los 7.449 que respondieron, 46% de las niñas declararon que habían recibido ese tipo de solicitaciones de un adulto.

Varios de los que respondieron señalaron haber recibido ese tipo de solicitaciones por Internet y otros conductos.

La cifra correspondiente para los niños varones fue de 16%. Se pedía a los adolescentes que se desnudasen frente a la cámara o que mirasen a un adulto masturbándose frente a su cámara.

Los adolescentes estudiados indicaron que esos incidentes eran comunes y que ocurrían a menudo en los sitios de charla.

Las solicitaciones mencionadas no eran en modo alguno sutiles; el adulto pedía servicios sexuales desde el principio de la conversación.

En ese mismo estudio se examinaron informes policiales de delitos contra niños cometidos a través de nuevas tecnologías y, en 50% de los casos, los delitos señalados sólo se producían en línea, donde las solicitudes de imágenes o de contactos por cámara web eran los más frecuentes.

[29] Mitchell, K.J., Finkelhor, D. and Wolak, J. *Youth Internet users at risk for the most serious online solicitations.* American Journal of Preventive Medicine, 32 (6), 2007, S32-S37.

[30] Ybarra, M.L., Leaf, P.J. and Diener-West, M. *Sex differences in youth-reported depressive symptomatology and unwanted Internet sexual solicitation.* Journal of Medical Internet Research, 6 (1), 2001, 9-18.

[31] Mitchell, K.J., Finkelhor, D. and Wolak, J. *Risk factors for and impact of online sexual solicitation of youth.* JAMA, 285 (23), 2001, 3011-3014.

Los demás delitos señalados se cometieron en la vida real, pero los contactos se habían establecido antes por Internet.

En la mitad de los delitos en el mundo real, la víctima se encontró con el autor sabiendo que el encuentro acabaría siendo sexual.

En los demás casos, la víctima pensaba que la naturaleza del encuentro sería totalmente diferente[32].

Recientes informes de víctimas de ese tipo de solicitaciones o de intentos de engatusamiento en Suecia confirmaron e infirmaron las conclusiones del estudio de New Hampshire.

En Suecia, en un caso que afectó a más de 100 niñas resultó evidente que todas ellas sabían que el encuentro con un hombre acabaría en encuentro sexual.

Sin embargo, ninguna de las niñas reconoció ser plenamente consciente de lo que ello entrañaba.

Con su comportamiento en las conversaciones, las niñas daban al perpetrador indicaciones sobre sus vulnerabilidades y le ofrecían la oportunidad de aprovecharlas aun antes de que las explotara sexualmente.

Las vulnerabilidades iban de la soledad a tendencias suicidarias. Las niñas iban solas a la cita con el perpetrador, pero no por ello eran víctimas consintientes[33].

Es evidente que el número de solicitudes de contactos en línea es considerable y que los adolescentes y niños los señalan y saben de qué se trata.

Si se observan los casos de delitos en línea y en la vida real, es evidente que la solicitud de que el o la adolescente envíe imágenes o participe en un encuentro sexual por cámara web suele marcar el inicio del abuso sexual.

En los últimos años se ha observado una inquietud creciente acerca de los tipos de comportamientos que pueden resultar peligrosos para los niños en los sitios de contactos sociales.

Analizaremos esta cuestión más adelante cuando examinemos las oportunidades que tienen los niños de adoptar comportamientos problemáticos en Internet, pero es interesante observar que en YISS-2, 16% de los niños reconocieron utilizar páginas personales (blogs) en el último año.

Los blogs contienen material creado por los usuarios de Internet y presentan algunas de las calidades de los sitios de contacto social.

Ahora bien, se ha descubierto que los adolescentes y las niñas son los usuarios más comunes de este tipo de servicios y tienen más probabilidades que los demás jóvenes de colgar información personal en línea[34].

No obstante, los blogueros no tienen más probabilidades de comunicar con personas que conocieron en línea y que no conocen en persona.

Los blogueros que no respondían a los contactos no tenían mayores riesgos de solicitaciones sexuales y colgar información personal no aumentaba los riesgos de por sí.

Lo cierto es que los blogueros corren más riesgos de ser acosados en línea, comuniquen o no con otros.

En la encuesta *UK Children Online* también se indica que los jóvenes que están menos satisfechos con su vida y conocen y utilizan más

[32] Brottsförebyggande Rådet. *Vuxnas sexualla kontakter med barn via Internet.* [Adults' sexual contacts with Children via the Internet] Report 2007:11. Brottsförebyggande Rådet. 2007. Stockholm.

[33] Wagner, K: Alexandramannen. Förlags AB Weinco. Västra Frölunda. 2008.

[34] Mitchell, K.J., Wolak, J. and Finkelhor, D. *Are blogs putting youth at risk for online sexual solicitation or harassment? Chid Abuse and Neglect*, 32, 2008, 277-294.

Internet tendrán tendencia a considerar que la red es un instrumento de comunicación, y pueden adoptar comportamientos más arriesgados[35].

Con la práctica y la experiencia, es probable que descubramos los factores que debemos cambiar para poder ayudar a los niños que han sido engatusados en línea para ser abusados sexualmente en la vida real.

Sabemos que el engatusamiento en línea es más rápido que en la vida real, y además puede ser anónimo: los niños confían más fácilmente en sus "amigos" en línea y tienden a desinhibirse más cuando comunican, y los agresores no están tan limitados por el tiempo o la accesibilidad como lo estarían en el mundo "real".

En general, los perpetradores se informan lo más posible sobre sus futuras víctimas, evalúan los riesgos y probabilidades de que los niños hablen de ese contacto, se informan sobre las redes sociales del niño, pueden facilitar información falsa sobre ellos mismos, como fotografías falsas, y, si lo consideran bastante seguro, establecen una "relación" con el niño, o tratan de controlarlo de modo que puedan darle una cita en la vida real[36].

BUP Elefanten, unidad psiquiátrica para niños y adolescentes que trata a los niños víctimas de abusos sexuales y físicos en Suecia, está investigando métodos terapéuticos para ayudar a los niños y adolescentes que han sido explotados en línea y en la vida real.

El proyecto está en marcha desde 2006 y ha entrevistado a más de 100 jóvenes, terapeutas, policías, representantes de ministerios públicos y trabajadores sociales.

Esos jóvenes han sido víctimas de diversos abusos tales como acoso sexual, sexo por la cámara web, divulgación de sus fotografías en Internet, encuentros en línea que conducen a abusos en la vida real y venta de sexo en línea por los propios niños[37].

Cuando se analizan los datos de estas entrevistas se observa que estos jóvenes se pueden dividir en tres grupos:

1. los que han sido engañados y han caído en trampas inesperadas;
2. los arriesgados, que corren riesgos para satisfacer sus necesidades emocionales y llamar la atención;
3. los autodestructores que, por ejemplo, venden sexo o se comprometen a sabiendas en relaciones abusivas.

Los integrantes de este último grupo son reacios a considerarse como "víctimas" y piensan más bien que controlan la situación.

Según los resultados de estos estudios clínicos, muchos de estos niños no quieren recibir ayuda, y es importante que los médicos no los abandonen y traten en cambio de mantener el contacto con ellos hasta que se sientan preparados para recibir algún tipo de ayuda.

[35] Livingstone, S. and Helsper, E.J. *Taking risks when communicating on the Internet. The role of offline social-psychological factors in young people's vulnerability to online risks*. Information, Communication and Society, 10 (5), 2007, 618-643.

[36] Palmer, T. *Just One Click*. London: Barnardos. 2004.

[37] Quayle, E., Lööf, L. & Palmer, T. (2008). *Child Pornography And Sexual Exploitation Of Children Online*. Bangkok: ECPAT International.

Uno de los principales objetivos del engatusamiento de los niños que son objeto de fotografías abusivas es que guarden silencio.

Este silencio se debe a que los jóvenes creen sinceramente que la persona que les había citado era su amigo y no están dispuestos a reconocer el tipo de conversación que han tenido en línea.

El primer motivo influencia la manera en que los jóvenes definen y determinan amistades, y el segundo se debe a que, como se ha indicado anteriormente, los jóvenes están mucho más desinhibidos cuando comunican en línea.

“Internet puede llevar a jóvenes y niños a prácticamente cualquier lugar del mundo y, por lo tanto, exponerlos a riesgos potenciales”

Acceso a material problemático en línea

Aunque sería simplista decir que el material pornográfico o de carácter sexual no existía antes de Internet, también es cierto que Internet ha facilitado el acceso prolífico a material sexual.

La accesibilidad, la interactividad y el anonimato de Internet son, precisamente, los factores que aumentan la probabilidad de encontrar material violento o sexual.

En el estudio SAFT, 34% de los niños han visto un sitio web violento, ya sea accidental o voluntariamente[38].

Los estudios del New Hampshire han puesto de manifiesto que los jóvenes se exponen accidentalmente a material sexual indeseado en Internet, pero también han reconocido que las investigaciones actuales en las cuales se estudian los efectos de esa exposición a material sexual indeseado se han llevado a cabo principalmente entre estudiantes y jóvenes adultos, en lugar de niños jóvenes, y que se ha tratado principalmente de exposición voluntaria más que accidental.

No existen muchos estudios que apoyen la idea de que los distintos tipos de adolescentes que quedan atrapados en relaciones de abuso y explotación en línea son los jóvenes arriesgados y autodestructivos que quizá también accedan a sitios pornográficos o de conversación destinados a adultos que buscan compañeros sexuales.

Según la encuesta YISS-1, 1 de cada 4 niños que utilizan regularmente Internet vieron imágenes de carácter sexual indeseadas durante el año anterior a la compilación de los datos. 73% de los casos se produjeron mientras los jóvenes buscaban o navegaban por Internet, y la mayoría en el propio hogar y no en la escuela.

Los autores también estudiaron cómo las técnicas de programación pueden mantener esa exposición y hacen muy difícil poder salir de ella. Esas "ratoneras" se observaron en la tercera parte de esos incidentes perturbadores.

La mayoría de los niños que estuvieron expuestos a ese tipo de material declararon que no habían quedado particularmente perturbados.

No obstante los autores insistieron en que ese tipo de exposición, en particular cuando no es deseada, puede afectar la actitud con respecto al sexo o a Internet y el sentido de seguridad y comunidad de los jóvenes.

Cuando se efectuó la encuesta YISS-2, se observó un aumento de la exposición indeseada a pornografía, en particular entre los niños de 10 a 12 años de edad, de 16 a 17 años de edad y jóvenes blancos no hispánicos[39].

En un estudio sobre los jóvenes australianos (16 a 17 años de edad), se observó que las tres cuartas partes habían sido expuestos accidentalmente a sitios web pornográficos, mientras que 38% de niños y 2% de niñas habían accedido voluntariamente a ellos[40].

Este estudio concluye que el comportamiento de los niños frente a la pornografía refleja el de los adultos.

En primer lugar, es más probable que un varón busque y sea un con-

[38] SAFT. *Safety Awareness Facts Tools.* Brussels: European Commission. Accessed 5.6.2007 from: http://ec.europa.eu/information_society/activities/sip/projects/awareness/closed_projects/saft/index_en.htm.

[39] Mitchell, K.J., Wolak, J. and Finkelhor, D. *Trends in youth reports of sexual solicitations, harassment, and unwanted exposure to pornography on the Internet.* Journal of Adolescent Health, 40, 2007, 116-126.

[40] Flood, M. *Exposure to pornography among youth in Australia.* Journal of Sociology, 43 (1), 2007, 45-60.

sumidor más frecuente de películas para adultos y sitios web pornográficos.

En segundo lugar, los usuarios de Internet de todas las edades tienen dificultades para evitar encuentros no deseados con materiales explícitamente sexuales.

Ejemplo de ello son algunos juegos informáticos que pueden tener contenido altamente sexual. Esos juegos están clasificados "para adultos" pero, inevitablemente, muchos jóvenes juegan con ellos.

También es importante señalar que ese tipo de exposición no es exclusiva de las nuevas tecnologías, y se produce también en medios más tradicionales como la televisión, donde las horas de difusión de material erótico y sexual puede coincidir con las horas en que los niños pueden estar frente al televisor.

Uno de los factores que puede revestir cierta importancia en este caso es el control de la exposición, y es posible que las consecuencias de una exposición accidental sean diferentes de las de una exposición voluntaria.

También se ha determinado que algunos menores quedan sorprendidos por el contenido de material que se encuentran por inadvertencia cuando navegan por Internet[41].

Un acceso imprevisto o parcial a cierto tipo de materiales puede ser un problema considerable y se ha sugerido que[42]: "Las tecnologías más recientes (incluido el vídeo, pero también Internet y las comunicaciones móviles) permiten ver contenido fuera de contexto.

Se puede ver por ejemplo una serie de avances en lugar del guión completo, con el que se comprendería el contenido. El contexto editorial siempre se ha considerado importante en las directrices de reglamentación del contenido (por ejemplo, BBFC, Ofcom), que podría ser difícil adaptar para elaborar directrices paralelas para los nuevos medios.

No obstante, de las investigaciones sobre la exposición accidental de niños a pornografía en Internet se desprende claramente que un contenido imprevisto y fuera de contexto puede ser particularmente perturbador. Esto plantea dificultades a los reguladores".

Ahora bien, no se han realizado muchos estudios sobre la utilización de pornografía por los jóvenes, y en la mayoría de los casos son los propios encuestados los que responden, por lo que las diferencias pueden deberse sencillamente a lo que las normas sociales prevalecientes dictarían al adolescente.

Puede decirse por supuesto que muchos niños y adolescentes declaran que sólo se toparon accidentalmente con material pornográfico, ya que consideran inapropiado confesar que lo buscaron activamente en Internet.

En Suecia, en una muestra representativa de adolescentes de 18 años de edad, 65% de los varones miraban pornografía cada mes, contra sólo 5% de mujeres. Cabe señalar que sólo 7% de los varones y 31% de las adolescentes que contestaron al estudio declararon que nunca miraban pornografía[43].

[41] Fug, O.C. *Save the children: The protection of minors in the information society and the audiovisual media services directorate*. Journal of Consumer Policy, 31, 2008, 45-61.

[42] Livingstone, S. and Hargrave, A.M. *Harmful to children? Drawing conclusions from empirical research on media effects*. In U. Carlsson (ed) *Regulation, Awareness, Empowerment. Young People and Harmful Media Content in the Digital Age*. Göttenborg: Nordicom. 2006.

[43] Mossige, S., Ainsaar, M. and Svedin, C.G. *The Baltic Sea Regional Study on Adolescent's Sexuality*. NOVA Rapport 18/07. Oslo: NOVA, s. 93-111

Muchos jóvenes están expuestos a material sexual en línea y hemos visto claramente que no todos los casos son accidentales o perjudiciales.

Una de las preocupaciones es que la exposición a material pornográfico anormal o violento puede tener consecuencias en las creencias y actitudes de algunos jóvenes y, en menor medida, en el comportamiento de unos pocos.

Esto se considera cada vez más como un posible problema de sanidad pública y parece que la consecuencia de ese tipo de exposición en un medio esencialmente desreglamentado como Internet es merecedor de investigaciones más pormenorizadas[44].

Oportunidades problemáticas

Otro de los peligros de las nuevas tecnologías estriba en los propios medios y en la oportunidad que tienen los jóvenes de adoptar comportamientos que pueden resultar preocupantes.

Puede tratarse de actividades de autovictimización a través de Internet y del teléfono móvil, aunque este término puede parecer problemático, ya que corresponde esencialmente a la capacidad creciente de generar contenido en línea.

Según diversos datos, la proporción de jóvenes de 11 a 16 años de edad que poseen un teléfono móvil es superior a la de adultos, ya que 76% de los niños tienen su teléfono propio[45].

[44] Perrin, P.C., Madanat, H.N., Barnes, M.D., Corolan, A., Clark, R.B., Ivins, N. et al. *Health educationa's role in framing pornography as a public health issue: local and national strategies with international implications*. Promotion and Education, 15, 2008, 11-18.

[45] Child-Wise Monitor (2002). Accessed on 18.06.07 at: http://www.childwise.co.uk/monitor.htm

En una encuesta realizada entre 1.340 alumnos de secundaria de la zona de Teesside en el Reino Unido en 2004, se determinó que 86% poseían un teléfono móvil (89,7% de niñas y 82,3% de niños)[46].

En ese estudio, la utilización de los teléfonos móviles se limitaba a llamadas telefónicas y textos, pero según los datos disponibles los teléfonos móviles se utilizan cada vez más para otros tipos de comunicaciones.

En el estudio *UK Children Go Online*, no obstante, parece que estas cifras se diversifican y que 38% de los jóvenes tienen un teléfono móvil, 17% un televisor digital y 8% una consola de juego, todos ellos con acceso a Internet.

Para muchos jóvenes, el teléfono móvil es un medio vital de comunicación y una manera de relacionarse con un amplio mundo social, y participar en él.

En 2007, el estudio cualitativo de la OPTEM realizado en 29 países europeos señaló que la gran mayoría de los niños tenían teléfono móvil.

No obstante, se expresan preocupaciones crecientes de que esas posibilidades tecnológicas puedan entrañar prácticas que puedan afectar a otros individuos o en las que intervengan los propios jóvenes.

Las imágenes o películas tomadas por el propio niño pueden considerarse parte del proceso de engatusamiento en el que el delincuente convence al niño o a la niña de que le envíe imágenes, ya sea desnudo o adoptando comportamientos sexuales.

Las imágenes se utilizan a menudo para convencer al menor de que los contactos sexuales entre niños y adultos son inofensivos, y disminuir así las inhibiciones del menor frente al sexo en línea o a un encuentro sexual pagado con el adulto.

Las víctimas son vulnerables por diversos motivos tales como soledad, intimidación o conflictos constantes con los padres. El adolescente se considera cómplice del abuso después de enviar las imágenes al adulto.

El grupo de la Universidad de New Hampshire también estudió la cuestión de los daños causados examinando los casos reunidos por 1.504 médicos para determinar los tipos de experiencias problemáticas señalados en relación con nuevas tecnologías.

Descubrieron once tipos de experiencias problemáticas señaladas por pacientes jóvenes y adultos.

Se trataba de: utilización abusiva, pornografía, infidelidad, explotación y abusos sexuales, juegos, juegos de azar y de roles, acoso, utilización para evitar el aislamiento, fraudes, robo y engaño, relaciones fallidas en línea, sitios web con influencias perjudiciales y utilización arriesgada e inapropiada[47].

En otro análisis se estudió qué experiencias problemáticas se identificaban como problemas primarios o secundarios[48].

Los problemas más probables que pueden tener jóvenes y adultos están relacionados con una utilización excesiva de Internet, la pornografía para adultos, la pornografía infantil, la explotación sexual y los juegos, los juegos de azar y los de roles.

Otros problemas relacionados con Internet, tales como su utilización para evitar el aislamiento, la

[46] Madell, D. and Muncer, S. *Back from the beach but hanging on the telephone? English adolescents' attitudes and experiences of mobile phones and the Internet.* CyberPsychology and Behavior, 7 (3). 2004, 359-367.

[47] Mitchell, K.J., Becker-Blease, K.A. and Finkelhor, D. *Inventory of problematic Internet experiences encountered in clinical practice. Professional Psychology: Research and Practice*, 36 (5), 2005, 498-409.

[48] Mitchell, K.J. and Wells, M. *Problematic Internet experiences: Primary or secondary presenting problems in persons seeking mental health care?* Social Science and Medicine, 65, 2007, 1136-1141.

explotación sexual, el acoso y la infidelidad en línea tienen las mismas probabilidades de ocurrir.

Entre los jóvenes que solicitaban ayuda psicológica, se observó que los juegos, juegos de azar y juegos de roles aumentaban 1,7 veces la probabilidad de comportamientos problemáticos, y que esa probabilidad era cuatro veces mayor entre los jóvenes víctimas de fraude u otro tipo de engaño en línea.

Es más probable que los jóvenes explotados sexualmente hayan sido diagnosticados con trastornos de estrés postraumático (PTSD, *Post Traumatic Stress Disorder*) que los jóvenes con otros problemas relacionados con Internet.

Intimidación

Ya hemos dicho que no debe considerarse que la intimidación en línea es diferente de la intimidación en la vida real. A veces la intimidación en línea o por teléfono móvil se califica de "ciberintimidación", pero este término no ayuda siempre a comprender lo que pasa en realidad. La intimidación es intimidación, se produzca donde se produzca.

Según el Byron Review del Reino Unido, "ciberintimidación es un comportamiento intimidatorio por medios electrónicos, como enviar textos amenazadores, colgar información desagradable sobre otras personas y divulgar imágenes o vídeos desagradables de otra persona".

La intimidación en línea o por teléfono móvil puede ser una prolongación de la intimidación personal, o puede ser una venganza por incidentes ocurridos en la vida real. La intimidación en línea o por teléfono móvil puede ser particularmente perturbadora y dañina porque se divulga más ampliamente, con mayor publicidad y el contenido distribuido electrónicamente puede volver a la superficie en cualquier momento, por lo que la víctima de la intimidación tendrá más dificultades para poner término al incidente; puede

contener imágenes perjudiciales o palabras perniciosas; el contenido es accesible las 24 horas del día, la intimidación por medios electrónicos puede producirse las 24 horas del día y los 7 días de la semana e invadir la vida privada de la víctima incluso en lugares "seguros" tales como el hogar, y la información personal se puede manipular, las imágenes se pueden alterar y después enviar a otras personas.

Además, se puede llevar a cabo anónimamente[49].

Esa actividad intimidatoria puede ser una simple tomadura de pelo o ser también muy agresiva, y según estudios de la Universidad de New Hampshire existen muchos puntos comunes entre actos ilegales, tales como el acoso sexual, y la intimidación.

En un estudio reciente en Alemania se estudiaron las perspectivas de las víctimas del comportamiento intimidatorio en salas de charla Internet[50].

Se identificaron varios tipos de intimidación tales como acoso, abuso, insultos, burlas y chantaje.

Esas intimidaciones eran frecuentes y a menudo las víctimas eran los mismos niños.

Es importante señalar que ese estudio también demostró que existe una relación entre las víctimas en la escuela y las víctimas en las salas de charla Internet.

Los adolescentes víctimas de intimidación en el colegio también tenían más probabilidades de ser víctimas en las salas de charla.

También se observó que era más probable que esos niños fueran menos populares y tuvieran menos confianza en sí mismos, y que era probable que los padres fueran sobreprotectores.

También se señala que esos niños pasaban de ser víctimas a intimidadores y que esto podía interpretarse como "venganza" o "desahogo".

Las víctimas de intimidación en las salas de charla Internet también señalaron que a menudo visitaban sitios en línea arriesgados y, de hecho, se ponían ellos mismos en condiciones de ser las víctimas.

El estudio señaló que, en comparación con víctimas de intimidaciones graves en la escuela, las víctimas de intimidaciones graves en salas de charla adoptan más frecuentemente comportamientos de manipulación social cuando visitan salas de charla (por ejemplo, dan información falsa sobre su edad o sexo).

En investigaciones entre niños de Estados Unidos se ha llegado a las conclusiones siguientes:

1. entre los usuarios frecuentes de Internet, la "ciberintimidación" es una experiencia común;
2. la intimidación en línea y en la escuela son similares y las experiencias tienen muchos puntos comunes en ambos contextos;
3. si bien algunos métodos y aparatos de comunicación electrónicos están asociados con un alto riesgo de "ciberintimidación", son simples herramientas, y no causas del comportamiento;
4. independientemente de la intimidación en la escuela, la ciberintimidación está asociada con un aumento de la angustia;
5. los jóvenes rara vez hablan a los adultos de la intimidación en línea y no aprovechan bien las herramientas que les ofrecen las tecnologías de la comunicación para impedir futuros incidentes[51].

[49] Byron, T. (2008). *Safer Children in a Digital World The Report of the Byron Review*. Available from http://www.dcsf.gov.uk/byronreview/pdfs/Final%20Report%20Bookmarked.pdf

[50] Katzer, C., Fetchenhauer,D. and Belschak, F. *Cyberbullying: Who Are the Victims? A Comparison of Victimization in Internet Chatrooms and Victimization in School*. Journal of Media Psychology 2009; Vol. 21(1):25–36.

[51] JUVONEN, J. & Gross, G.F. *Extending the School Grounds?—Bullying Experiences in Cyberspace*. Journal of School Health, 2008, 78 (9), 496 – 505.

4. Guía para padres, tutores y educadores

Los consejos de seguridad se basan en el análisis de los datos reunidos y las investigaciones disponibles. Esta sección tiene por objeto reunir consejos para padres, tutores y educadores a fin de ayudarlos a enseñar a sus niños a tener un comportamiento seguro, positivo y enriquecedor en línea.

Los padres, tutores y educadores deben tener en cuenta la naturaleza exacta de cada sitio web, el sentido del peligro de sus niños y la probabilidad de que el adulto pueda reducir los riesgos, antes de decidir qué entorno es apropiado para el niño.

Internet ofrece incontables posibilidades de emancipar a niños y jóvenes y ayudarlos a descubrir cosas por sí mismos. Enseñarles un comportamiento en línea positivo y responsable es fundamental.

Padres, tutores y educadores			
	#	Principales consideraciones	Descripción
Seguridad y protección de su ordenador personal	1.	Tener el ordenador en una sala común	Puede ser muy importante tener el ordenador en una sala común y estar presente, especialmente cuando niños más jóvenes utilizan Internet. Si no puede estar presente, contemple otras posibilidades de vigilar estrechamente lo que hacen los niños en línea, utilizando por ejemplo medios técnicos. En las familias más numerosas la multiplicidad de ordenadores puede crear ciertos límites prácticos que también se plantean si se insiste en que todos estén en la misma habitación todo el tiempo, y recuerde que cuando los niños crecen tienen derecho a cierta privacidad. Más y más niños adquieren ordenadores personales y las redes inalámbricas se están generalizando en los hogares, por lo que será también más difícil mantener reglas de este tipo.
	2.	Instalar programas cortafuegos y antivirus	Asegúrese de que su ordenador tiene instalados programas cortafuegos y antivirus y que están al día. Inculque al niño los fundamentos de la seguridad en Internet.
Reglas	3.	Adoptar reglas sobre la utilización de Internet y de aparatos personales en casa, prestando particular atención a las cuestiones de privacidad, edad, lugares inapropiados, intimidación y el peligro que representan los extraños	En cuanto el niño empieza a utilizar Internet, estudiar y elaborar una lista de reglas. Esas reglas deben referirse también al tiempo de utilización de Internet y al tipo de utilización.
	4.	Determinar reglas de utilización de aparatos móviles	En cuanto el niño empieza a utilizar un teléfono móvil, estudiar y elaborar una lista de reglas. Esas reglas deben estipular si el niño puede utilizar o no el teléfono móvil para navegar por Internet y la frecuencia con que puede utilizarlo, qué tipo de material pueden adquirir o telecargar con el teléfono, qué hacer con las cosas inapropiadas, y los niveles de gastos.

Padres, tutores y educadores			
	#	Principales consideraciones	Descripción
Educación de padres, tutores y maestros	5.	Los padres deben familiarizarse con los sitios Internet que utilizan los niños (por ejemplo, servicios y productos ofrecidos por sitios Internet) y tener un buen conocimiento de cómo pasan su tiempo en Internet	Evaluar los sitios que quieren utilizar los niños y leer cuidadosamente la política de privacidad, las condiciones de utilización y los códigos de conducta (que a menudo se llaman "reglas de la casa"), así como las páginas que pueda haber para los padres. Además, buscar si el sitio supervisa el contenido colgado en las páginas de los servicios y vigilar periódicamente la página del niño. Comprobar si ese sitio vende productos en línea.
	6.	Investigar recursos en línea para obtener información adicional sobre la seguridad en línea y cómo utilizar Internet de manera positiva	Cada año se celebra la utilización positiva y más segura de Internet. Pueden participar niños, escuelas locales, empresas privadas y actores del ramo que colaboran para lograr una mayor sensibilización sobre las oportunidades de promover una experiencia en línea positiva. Para consultar la información más reciente sobre estos eventos, busque en línea expresiones como "celebración de la seguridad de Internet" + "nombre del país".
	7.	Comprender cómo los niños utilizan otros aparatos personales tales como teléfonos móviles, consolas de juego, lectores MP3 y PDA	Hoy se puede acceder a Internet a través de diversos otros aparatos personales que, por lo tanto, pueden plantear problemas de seguridad similares.

	#	Principales consideraciones	Descripción
Examen de las características de los sitios Internet	8.	Determinar si filtrar y bloquear o supervisar programas puede ayudar a apoyar o respaldar la utilización segura de Internet y de aparatos personales por niños y jóvenes. Si recurre a ese tipo de programa, explíquele al niño lo que hace y por qué. Mantenga secretas las contraseñas de esos programas	Se pueden plantear cuestiones de confianza y del derecho del joven a la privacidad cuando se utilizan medios técnicos, en particular programas de supervisión. En circunstancias normales, conviene que el padre o tutor comente los motivos que le impulsan a utilizar ese tipo de programa, y también debería explicarse cuidadosamente su utilización en las escuelas.
	9.	Consentimiento parental	Algunos países, como España y Estados Unidos, disponen de leyes en las que se especifica la edad mínima a la cual una empresa o un sitio web puede pedir a un joven que facilite información personal sin haber obtenido previamente un consentimiento verificado de los padres. En España son 14 años y en Estados Unidos 13. En otros países se considera apropiado exigir el consentimiento parental antes de pedir datos personales a los jóvenes. Muchos sitios destinados a los niños más jóvenes piden el consentimiento parental antes de admitir a un nuevo usuario. Compruebe cuáles son esas exigencias en los sitios a los cuales quiere inscribirse el niño.
	10.	Controlar la utilización de tarjetas de crédito y otros medios de pago	Controlar la utilización de líneas fijas o teléfonos móviles para adquirir bienes virtuales. La tentación puede ser demasiado grande cuando los niños pueden utilizar líneas fijas o teléfonos celulares para adquirir cualquier tipo de bienes o servicios. Además, mantenga sus tarjetas de crédito y débito en lugar seguro y, por supuesto, sus números de identificación personal.
	11.	Asegúrese de que se pide la edad cuando se adquieren bienes y servicios en línea	Normalmente no se comprueba la edad cuando se adquieren mercancías, pero están apareciendo sistemas que garantizan la comprobación de la edad en el punto de venta. En todos los casos, siga cuidadosamente los gastos del niño en línea.

	#	Principales consideraciones	Descripción
	12.	Compruebe si el sitio Internet tiene un moderador	Asegúrese de que el sitio Internet modera las conversaciones, preferiblemente con filtros automáticos y supervisores humanos. ¿Comprueba el sitio todas las fotografías y los vídeos que se cuelgan?
	13.	Bloquee el acceso a contenidos o servicios indeseables	Los medios técnicos también podrán ayudarle a bloquear el acceso a sitios web indeseables, por ejemplo los que autorizan contenidos o conversaciones no moderados, o a bloquear el acceso a servicios o contenidos indeseables en teléfonos móviles.
	14.	Comprobar la flexibilidad de los contratos	Compruebe cómo suprimir una cuenta, aunque entrañe la pérdida del precio de suscripción. Si el servicio no permite suprimir una cuenta, contemple la posibilidad de no utilizarla o de bloquear el acceso. Señale esa imposibilidad a las autoridades locales.
	15.	Estudie el alcance del servicio	Analice las políticas del proveedor de contenido y su cumplimiento, mire el contenido y los servicios ofrecidos y sea consciente de las limitaciones técnicas (por ejemplo, los anuncios publicitarios pueden no estar claramente identificados como tal).
	16.	Mire las publicidades y señale las publicidades inapropiadas	Fíjese en los anuncios y señale a la autoridades competentes anuncios que: 1. Inducen a error simplificando demasiado cuestiones complejas. 2. Incitan a los niños a hablar con extraños o ir a lugares peligrosos. 3. Muestran personas, en particular niños, que utilizan cosas peligrosas o están cerca de cosas peligrosas. 4. Fomentan una emulación insegura o comportamientos peligrosos. 5. Fomentan la intimidación. 6. Causan daños morales y temor a los niños. 7. Fomentan malos comportamientos alimentarios. 8. Aprovechan la credulidad de los niños.

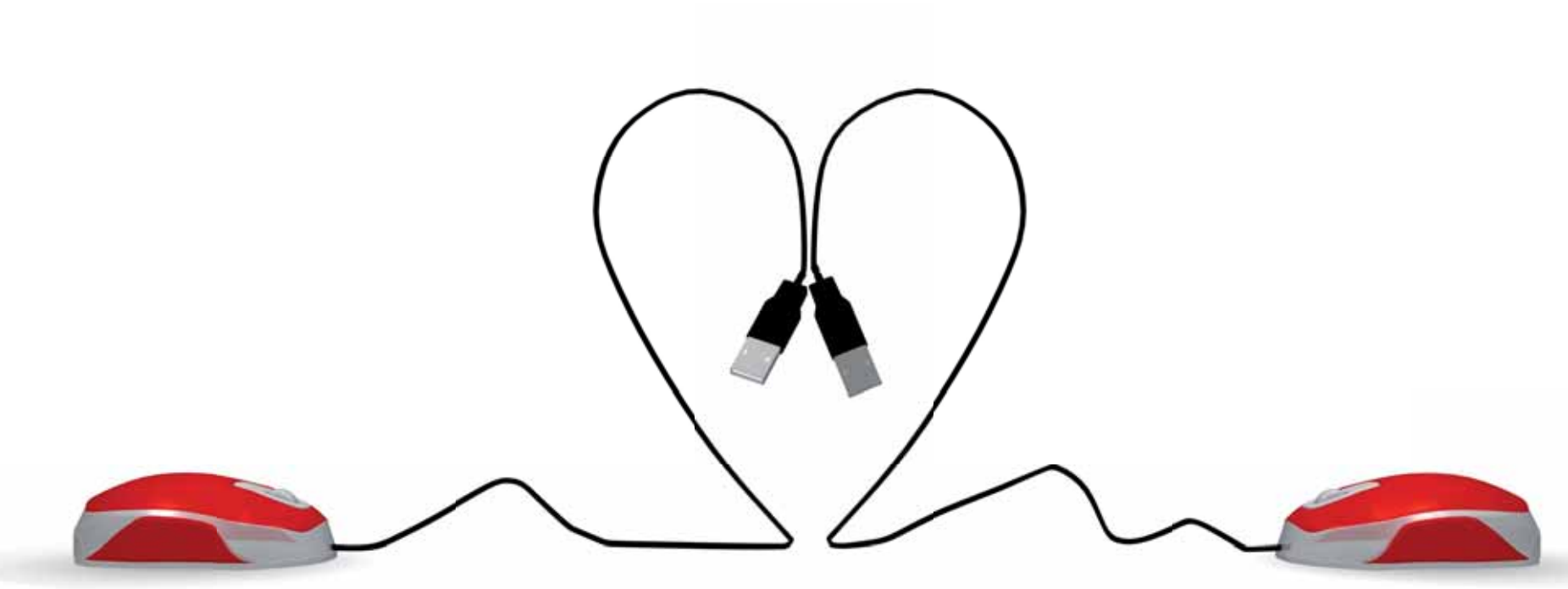
	#	Principales consideraciones	Descripción
Educación de los niños	17.	Eduque a los niños	La educación y el conocimiento del medio utilizado son fundamentales. Explique las normas y reglas del mundo virtual. Es probable que los niños acepten las directrices y, a menudo, recuerden a otros que hagan lo mismo. Enseñe a los niños a no responder a mensajes groseros y a evitar las conversaciones sexuales en línea. Enséñeles a no abrir ninguna pieza adjunta o enlace que reciban cuando conversan con otros, porque su contenido puede ser perjudicial.
	18.	Explique a los niños que no deben organizar nunca un encuentro personal con alguien que han conocido en línea	Los niños pueden correr un gran peligro si se reúnen con extraños que han conocido en línea. Los padres deben alentar a los niños a utilizar los sitios Internet únicamente para comunicar con sus amigos de la vida real, y no con los que nunca han visto en persona. Las personas en línea pueden no ser quienes dicen que son. No obstante, si el niño traba una fuerte amistad en línea y desea organizar un encuentro, en lugar de arriesgarse a que vaya solo o sin acompañante, deje claro que prefiere ir con él, o que vaya un adulto de confianza, y asegúrese de que el primer encuentro es en un lugar público bien iluminado y muy concurrido.
	19.	Impida al niño que divulgue información personal identificable	Ayude al niño a comprender qué información debe mantener secreta. Explique que los niños sólo deben colgar información que a usted y a él le parece conveniente que vean otros. Recuerde al niño que, una vez colgada, la información en línea no se puede quitar.
	20.	Asegúrese de que el niño comprende lo que significa colgar fotografías en Internet y utilizar webcams	Explique al niño que las fotografías pueden revelar mucha información personal. Los niños no deben poder utilizar webcams o colgar contenido alguno sin la aprobación de un padre, tutor o adulto responsable. Aliente a los niños a no colgar fotografías de ellos mismos o de sus amigos con detalles claramente identificables tales como nombres de calles, matrículas de automóviles, o el nombre de la escuela en la camiseta.
	21.	Prevenga al niño acerca de la divulgación de sus emociones a extraños	Los niños no deben comunicar directamente en línea con extraños. Explique que cualquiera que tenga acceso al mismo sitio puede leer lo que escriben y que los predadores o intimidadores a menudo buscan niños que se declaran interesados por trabar nuevas amistades en línea.

	#	Principales consideraciones	Descripción
Estudio de la utilización segura de sitios Internet	22.	Compruebe la página o el perfil del niño	Visite periódicamente la página del niño. Entre en la página y compruebe el historial de la cuenta del niño y, en caso necesario, ponga las opciones de charla a un nivel que le parezca adecuado. Los sitios Internet bien concebidos le ofrecen la oportunidad de participar muy activamente en la experiencia del niño. Si el niño se niega a respetar las reglas del sitio, puede contemplar la posibilidad de ponerse en contacto con el sitio y pedir que se supriman las páginas y el perfil del niño. Entre otras cosas, esto puede dar más peso a lo que le dice al niño sobre la importancia de las reglas y las consecuencias de su incumplimiento.
	23.	Asegúrese de que el niño respeta los límites del sitio Internet	Si el niño es menor de la edad recomendada por los sitios Internet, no le deje utilizarlos. Es importante recordar que los padres no pueden esperar que el proveedor de servicio pueda impedir que los niños menores de la edad estipulada puedan conectarse al sitio.
	24.	Asegúrese de que el niño no utiliza su nombre completo	Siempre que sea posible, el niño debe utilizar un apodo en lugar de su nombre real o parte del mismo. Los apodos se deben elegir con cuidado para no llamar indebidamente la atención. No autorice al niño a indicar el nombre completo de sus amigos o cualquier otra información que pueda facilitar su identificación, como el nombre de la calle en la que viven, su escuela, el número de teléfono, club de deportes, etc.
Comunicación	25.	Comunique con el niño sobre sus experiencias	Hable periódicamente al niño de los sitios que visita y con quién habla cuando está en línea. Anímelo a decirle si algo que ha visto en Internet le hace sentir incómodo o amenazado. Recuérdele que debe parar inmediatamente lo que esté haciendo si se siente incómodo o abriga alguna sospecha. Asegúrele que no tendrá problemas si le señala algo. A su vez, usted, como padre y adulto, no debe reaccionar violentamente cuando el niño comparte experiencias con usted. Mantenga la calma en cualquier circunstancia, infórmese de lo ocurrido y tome medidas. Felicite al niño por confiar en usted. Asegúrese de que el niño puede señalar los abusos.

Educadores[52]			
		Principales consideraciones	**Descripcióon**
Seguridad y protección forman parte de la estrategia de defensa de los niños	1.	Todos los miembros del establecimiento deben ser responsables de la ciberseguridad	Es importante que, incluso si las escuelas no permiten la utilización de ciertas tecnologías dentro del establecimiento, enseñen a los alumnos cómo comportarse de manera sensata y apropiada cuando las utilizan, e informarles sobre los riesgos.
	2.	Elaborar una política de utilización aceptable (PUA)	Debe detallarse cómo el personal, los alumnos y todos los usuarios de la red (incluidos los padres) pueden utilizar y no deben utilizar las instalaciones TIC.
Reglas y políticas	3.	Ejemplos de PUA pueden consultarse en línea y a través de las autoridades locales	Es importante adaptar esas reglas al contexto particular del establecimiento.
	4	Vincular las PUA con otras políticas del establecimiento	Se trata, entre otros, de políticas contra la intimidación y orientaciones sobre derechos de autor y plagio.
	5.	Punto de contacto único	Designar a un miembro veterano del equipo de gestión que sea responsable de la protección para que también sea el punto de contacto central en todo lo tocante a la ciberseguridad.
	6.	Necesidad de liderazgo	Los directores de colegios, apoyados por los miembros del consejo escolar, deben ser los primeros en llevar a la práctica las políticas acordadas en materia de ciberseguridad.
Sea integrador	7.	Mantener informados a los jóvenes	Asegúrese de que los jóvenes a su cargo son conscientes de los riesgos potenciales y de cómo adoptar un comportamiento seguro y responsable siempre que estén en línea.
	8.	Fomentar la resistencia	Permitir que los jóvenes definan sus propias estrategias de protección para cuando no dispongan de la supervisión y la protección tecnológica de un adulto.
	9.	Fomente la denuncia de agresiones y la adopción de responsabilidades	Ayude a los jóvenes a comprender que no son responsables de comportamientos ajenos que se les puedan imponer, pero que la escuela impondrá sanciones si se comportan de manera apropiada en línea.

[52] BECTA (2008) *Safeguarding children online.* Una guía para directores de escuelas puede consultarse en: www.becta.org.uk/schools/safety

		Principales consideraciones	Descripción
Soluciones tecnológicas	10.	Prácticas de auditoría	Asegurarse de que las medidas y soluciones tecnológicas se revisan y actualizan periódicamente para asegurar el mantenimiento de un programa eficaz de ciberseguridad.
Política de seguridad en Internet	11.	Formar a los maestros sobre políticas de seguridad Internet	Formar a los maestros sobre seguridad en Internet para ayudarlos a inculcar a los niños un comportamiento seguro en Internet.
	12.	Enseñar a los estudiantes a no dar nunca información personal cuando comunican con otros	Informar a los estudiantes de que nunca deben dar información personal (por ejemplo, nombre completo, dirección postal, dirección de correo electrónico, número de teléfono, nombre de la escuela, etc.) cuando comunican con extraños en línea.
	13.	Exigir que los estudiantes sólo busquen información específica	Exigir que los estudiantes busquen información específica y no "naveguen" al azar por Internet, y que registren en formato bibliográfico las URL de los sitios que utilizan.
	14.	Visite o pruebe los sitios web antes de enviar enlaces a los estudiantes	Visite personalmente cualquier sitio antes de recomendarlo a los estudiantes. También es una buena idea marcar las direcciones de los sitios antes de invitar a los estudiantes a visitar las URL.



5. Conclusiones

Las tecnologías de la información y la comunicación, o TIC, han transformado la vida del hombre moderno. Ofrecen comunicaciones en tiempo real, acceso sin fronteras y casi ilimitado a la información, e incontables servicios innovadores,

Por otra parte, también han creado nuevas oportunidades de explotación y abuso. Sin las protecciones apropiadas, los niños, que son grandes usuarios de Internet, corren el riesgo de ver imágenes violentas, sexuales o simplemente perturbadoras.

Si no nos dedicamos realmente a crear un ciberentorno seguro, decepcionaremos a nuestros niños. Si bien todos estamos mejor sensibilizados sobre los riesgos que entraña una utilización insegura de las TIC, todavía queda muchísimo por hacer.

Por consiguiente, es fundamental que padres y educadores puedan decidir, con el niño, lo que es una utilización apropiada y segura, y cómo comportarse de manera responsable con las TIC.

Si colaboran, padres, educadores y niños pueden cosechar los beneficios de las TIC y reducir lo más posible los peligros para los niños.

Esperamos que esta Guía le haya facilitado información clara y completa sobre la protección de la infancia en línea, los riesgos que pueden correr los niños y lo que padres y educadores pueden hacer para protegerlos y ayudarlos a comprender cómo cosechar los numerosos beneficios de las TIC reduciendo al mínimo los peligros potenciales.

Referencias y lecturas adicionales

Children's Online Privacy Protection Act (COPPA) http://www.coppa.org/coppa.htm

Cyberpeace Initiative, en la dirección: http://www.smwipm.cyberpeaceinitiative. org

Cyril. A. Wantland, Subhas C. Gupta, Scott A. Klein, *Safety considerations for current and future VR applications*, en la dirección: http://www.webmed.com/i-med/mi/safety.html (última visita el 4 September 2008).

'Are ads on children's social networking sites harmless child's play or virtual insanity?', The Independent, 2 de junio de 2008, en la dirección: http://www.independent.co.uk/news/media/are-ads-on-childrens-social-networking-sites-harmless-childs-play-or-virtual-insanity-837993.html (última visita el 11 de junio de 2008).

'Children's social-networking sites: set your little monsters loose online', Telegraph.co.uk, 17 de noviembre de 2007, en la dirección: http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2007/11/17/dlchildren17.xml (última visita el 10 de junio 2008).

CBC News, *Cyber-bullying*, 2005, en la dirección: http://www.cbc.ca/news/background/bullying/cyber_bullying.html (última visita el 4 de septiembre de 2008).

Child Exploitation and Online Protection Centre (CEOP): Think You Know, en la dirección: http://www.thinkuknow.co.uk/parents/gaming/bad.aspx (última visita el 4 September 2008).

Children, Adolescents, and Television, American Academy of Pediatrics, Pediatrics, Vol. 107, N° 2, febrero de 2001, en la dirección: http://aappolicy.aappublications.org/cgi/content/full/pediatrics;107/2/423 (última visita el 10 de septiembre de 2008).

Cyber-bullying: Developing policy to direct responses that are equitable and effective in addressing this special form of bullying, Canadian Journal of Educational Administration and Policy, Issue n. 57, 18 de diciembre de 2006, en la dirección: http://www.umanitoba.ca/publications/cjeap/articles/brown_jackson_cassidy.html (última visita el 2 de septiembre de 2008).

eModeration, Virtual World and MMOG Moderation: Five techniques for creating safer environments for children, mayo de 2008, en la dirección: http://www.emoderation.com/news/press-release-virtual-world-and-mmog-whitepaper (última visita el 22 de julio de 2008).

Entertainment & Leisure Software Publishers Association (ELSPA), Unlimited learning –Computer and video games in the learning landscape, en la dirección: http://www.elspa.com/assets/files/u/unlimitedlearningtheroleofcomputerandvideogamesint_344.pdf (última visita el 26 de agosto de 2008).

ENISA, Children on virtual worlds - What parents should know, septiembre de 2008, en la dirección: http://www.enisa.europa.eu/doc/pdf/deliverables/children_on_virtual_worlds.pdf

Gauntlett, David and Lizzie Jackson, *Virtual worlds – Users and producers, Case study: Adventure Rock*, Communication and Media Research Institute (CAMRI), University of Westminster, UK, en la dirección: http://www.childreninvirtualworlds.org.uk/pdfs/Gauntlett_and_Jackson_May_2008.pdf

Home Office, *Home office task force on child protection on the internet – Good practice guidelines for the providers of social networking and other user interactive services 2008*, 2008, en la dirección: http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-

guidance?view=Binary (última visita el 16 de junio de 2008).

Home Office, *Good practice guidance for the providers of social networking and other user interactive services 2008*, en la dirección: http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance (última visita el 12 de septiembre de 2008).

Home Office, *Good Practice Guidance for the Moderation of Interactive Services for Children*, en la dirección: http://police.homeoffice.gov.uk/publications/operational-policing/moderation-document-final.pdf (última visita el 12 de septiembre de 2008).

http://disney.go.com/fairies/pixiehollow/comingSoon.html (última visita el 26 de agosto de 2008).

http://www.redherring.com/Home/24182 (última visita el 10 julio de 2008).

Internet Watch Foundation: Protection Online http://www.iwf.org.uk/public/page.36.htm

Keith, Stuart, *'SpongeBob is the real threat to our children online'*, The Guardian, abril de 10, 2008, en la dirección: http://www.guardian.co.uk/technology/2008/apr/10/games.news (última visita el 10 de julio de 2008).

Kirriemuir J., *A Survey of the Use of Computer and Video Games in Classrooms*, Nesta Futurelab Series, 2002, en la dirección: http://ccgi.goldingweb.plus.com/blog/wp-content/Games_Review1.pdf (última visita el 2 de septiembre de 2008).

Kramer, Staci D., Disney Acquires Club Penguin; $350 Million Cash, Possible $350 Million Earnout, paidContent.org, 1 de agosto de 2007, en la dirección: http://www.paidcontent.org/entry/419-disney-acquires-club-penguin-in-deal-values-at-700-million-to-be-brande/ (última visita el 10 julio de 2008).

Mediashift, *Virtual Worlds for Children Entwined with Real World*, en la dirección: http://www.pbs.org/mediashift/2007/06/your_take_roundupvirtual_world.html (última visita el 28 de agosto de 2008).

Microsoft, *How to help your children' use social networking Web sites more safely*, 9 de noviembre de 2006, en la dirección: http://www.microsoft.com/protect/family/activities/social.mspx (última visita el 11 de junio de 2008).

NSPCC: Children and the Internet http://www.nspcc.org.uk/whatwedo/mediacentre/mediabriefings/policy/children_and_the_internet_media_briefing_wda49338.html

The Children's Charity: Net Smart Rules http://www.nch.org.uk/information/index.php?i=135

Virtual Worlds Management, *Disney.com Launches Games and Virtual Worlds Portal*; Mobile Widgets, 14 de agosto de 2008, en la dirección: http://www.virtualworldsnews.com/2008/08/disneycom-launc.html (última visita el 26 de agosto de 2008).

Virtual Worlds Management, *Virtual Worlds Managements Youth Worlds Analysis*, 22 de agosto de 2008, en la dirección: http://www.virtualworldsmanagement.com/2008/youthworlds0808.html (última visita el 25 de agosto de 2008).

Virtual Worlds News, *Virtual World 125,000 Children Fight Obesity in Whyville,* en la dirección: http://www.virtualworldsnews.com/2007/06/virtual_world_h.htm (última visita el 4 de septiembre de 2008).

Programas embajadores, para formar a capacitadores -varios nodos tienen buenos ejemplos. http://www.thinkuknow.co.uk/teachers/training.aspx, http://www.saferinternet.at/tipps/fuer-eltern/

Materiales docentes. Muchos excelentes recursos disponibles para divulgar mensajes de ciberseguridad. Las listas siguientes no son exhaustivas, y se pueden encontrar recursos adicionales en la dirección: http://www.saferinternet.org/ww/en/pub/insafe/resources.cfm.

http://www.digizen.org/cyberbullying/film.aspx un excelente recurso utilizado por varios nodos para combatir la intimidación.

http://www.internetsanscrainte.fr/le-coin-des-juniors/dessin-anime-du-mois Vinz et Lou – varios dibujos animados franceses para aumentar la sensibilización sobre cuestiones de ciberseguridad.

http://www.cyberethics.info/cyethics2/page.php?pageID=25&mpath=/35 ofrece numerosos trucos a los maestros.

http://www.easy4.it/content/category/13/59/104/ materiales del nodo italiano destinados a ayudar a los maestros.

http://www.teachtoday.eu/en/Lesson-Plans.aspx este sitio contiene varios planes de lecciones concebidos para las escuelas. El sitio se está actualizando y pronto habrá más información disponible.

http://dechica.com juego de sensibilización para niños pequeños desarrollado por el nodo búlgaro.

www.microsoft.com/cze/athome/bezpecnyinternet – versión flash del entretenido folleto sobre cómo utilizar Internet con más seguridad publicado por Microsoft. Promovido durante el Día 2009 para un Internet más seguro.

www.tietoturvakoulu.fi – Utilización más segura de Internet y prueba "Sé inteligente en la web".

Videoentrevistas con celebridades lituanas que dan su opinión y relatan experiencias personales de intimidación en línea. Idioma(s): letón. Más entrevistas: Vídeo 2 (estrella de la TV):

http://www.youtube.com/watch?v=QttMrRABnR0&feature=related Vídeo 3 (bailarín):

http://www.youtube.com/watch?v=3cPRlhQDJAg&feature=related Vídeo 4 (piloto de rally):

http://www.youtube.com/watch?v=PodsmBjrE6Y&feature=related Vídeo 5 (político):

http://www.youtube.com/watch?v=4_xrUvDQaIY&feature=related Vídeo 6 (cantante):

http://www.youtube.com/watch?v=usqpmAHjHQ4

www.tietoturvakoulu.fi los padres pueden probar su cultura mediática con esta prueba en línea sobre el sitio web. Idiomas: finlandés y sueco.

http://www.medieradet.se/Bestall--Ladda-ner/filmrummet una parte del sitio web del Consejo Sueco para los Medios está dedicado a imágenes en movimiento. Idioma(s): sueco y partes en inglés.

http://www.lse.ac.uk/collections/EUKidsOnline/ investigación europea sobre cuestiones culturales, contextuales y riesgos, en la utilización segura de Internet y de los nuevos medios por los niños.

http://www.nortononlineliving.com/ resume las tendencias en varios países.

http://www.pewinternet.org/ Pew facilita numerosos informes sobre la utilización de Internet y tecnologías conexas. Aunque se refiere a Estados Unidos, ha quedado demostrado que, con el tiempo, las tendencias observadas en Estados Unidos tienden a migrar hacia la UE.

http://www.unh.edu/ccrc/ investigación de David Finkelhor sobre las tendencias en las detenciones de predadores Internet, según la cual no existen pruebas reales que apoyen las afirmaciones de que Internet ha creado más predadores.

http://www.webwise.ie/article.aspx?id=10611 investigación realizada por el nodo irlandés.

http://www.childnet-int.org/young-people/

www.kidsmart.org.uk

www.chatdanger.com

Apéndice 1

Protección incorporada

Los PC y Mac tienen controles parentales incorporados en sus sistemas operativos y en sus sistemas más recientes (Windows Vista y Leopard de Mac). Si piensa actualizar su sistema operativo, ese cambio podría ahorrarle el coste de programas de vigilancia adicionales.

Para utilizar los controles de su ordenador, empiece por crear cuentas de usuario para cada uno de los niños. Consulte la guía de usuario del ordenador si no está seguro de cómo hacerlo.

Usuarios de Mac: a continuación, elija preferencias de sistema en el menú Apple, y pulse Cuentas. Para la cuenta de cada niño, pulse Controles Parentales y aparecerá una lista de categorías (correo, safari, etc.) que puede limitar o supervisar.

Si utiliza Leopard, puede registrar conversaciones IM y designar con quién puede hablar el niño por correo electrónico o iChat, entre otras cosas. También puede limitar los horarios. Por ejemplo, puede configurar el ordenador para que cierre automáticamente las cuentas de los niños a las 20.00 horas.

Usuarios de Windows: el acceso a los controles parentales se efectúa a través del panel de control. Busque Cuentas de Usuario y Panel de Control de seguridad familiar. Con Windows Vista, podrá elegir restricciones web y también podrá optar por recibir informes sobre la utilización del ordenador por el niño. Puede prohibir su utilización durante ciertas horas y bloquear videojuegos y programas censurables.

En todos los sistemas, la mayoría de los navegadores (Safari, Firefox, etc.) tienen un registro automático de historial que muestra los sitios visitados. Si no está familiarizado con el sistema, consulte el manual de usuario para ver cómo consultar ese historial. Compruebe todos los navegadores de su ordenador si tiene más de uno. Y tenga cuidado: los niños pueden aprender cómo suprimir el historial para borrar sus rastros; no dude en hacer preguntas si descubre que el historial ha sido limpiado por otra persona que usted.

¿Necesita más ayuda? Apple (Macs) y Microsoft (Windows) tienen programas didácticos en línea e información detallada en sus sitios web. Basta con buscar en Google "controles parentales" y "Apple" o "Microsoft" para encontrarlos.

Tenga siempre en cuenta que, por supuesto, por mucho que proteja a los niños, nunca será suficiente. Debe comunicar con ellos lo más posible y hablarles de la protección de la infancia en línea.

Apéndice 2

Descodificación de lenguaje instantáneo

Las abreviaturas y palabras codificadas aceleran la redacción de mensajes instantáneos y textos, pero también ocultan lo que se dice. Prepárese. Éstos son algunos de los términos comúnmente utilizados:

ADIH: Another day in hell (*Otro día en el infierno*)

A/S/L: Age, sex, location (*Edad, sexo, ubicación*)

BTDT: Been there done that (*Me conozco el percal*)

CULTR: See you later (*Nos vemos más tarde*)

GTFO: Get the f-ck out (*Expresion de sorpresa*) (*Sal de aquí*)

H8: Hate (*Odio*)

ILY o 143 o <3: I love you (*Te quiero*)

JK o J/K: Just kidding (*Estoy bromeando*)

KWIM: Know what I mean? (*Ya sabes lo que quiero decir*)

LLS: Laughing like sh-t (*Me parto de risa*)

LMIRL: Let's meet in real life (*Veámonos en la vida real*)

LYLAS (B): Love you like a sister (brother) (*Te quiero como una hermana/un hermano*)

NIFOC: Naked in front of computer (*Desnudo(a) frente al ordenador*)

PAW o PIR o P911: Parents are watching or Parent in room (drop the subject) (*Padres mirando o padres en la habitación (deja el tema)*)

POS: Parent over shoulder (can also mean "piece of sh-t," used as insult) (*Padre encima del hombro*)

Pr0n: Intentional misspelling of "porn" (*Mala ortografía voluntaria de "porn"*)

STFU: Shut the f-ck up (expression of surprise rather than reprimand) (*cállate de una vez*)

TMI: Too much information (*Demasiada información*)

TTFN: Ta ta, for now (goodbye) (*Hasta luego*)

WTF: What the f-ck? (*No entiendo nada*)

Fuente: http://www.parenting.com/article/Mom/Relationships/How-to-Spy-on-Your-Child-Online/3

Derechos de las fotografías: www.shutterstock.com, Violaine Martin/UIT, Ahone Ayeh Njume-Ebong/UIT

Unión Internacional de Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza
www.itu.int/cop

Impreso en Suiza
Ginebra, 2009

En colaboración con:

CHIS

THE UNIVERSITY OF EDINBURGH

ins@fe

CYBER Peace Initiative

enisa European Network and Information Security Agency