INTERNET SEGURA: FILTROS, BUSCADORES Y NAVEGADORES INFANTILES

Santiago Ferrer Marqués

Nos encontramos en un mundo real cubierto de una densa capa digital que llega a todas partes. La tecnología impregna toda nuestra realidad social, productiva, educativa y de ocio. Las TICs (Tecnologías de Comunicación e Información) se extienden de tal manera que es imposible substraerse a sus efectos.

Estos efectos, positivos o negativos, son tan reales y omnipresentes que han llegado a cambiar nuestra forma de producir, de relacionarnos, de comunicarnos, de entretenernos, de educarnos, y hasta de pensar. Las nuevas generaciones son generaciones digitales, porque lo han mamado desde la cuna. A ellos no les es difícil adaptarse a este mundo digital porque es el único que han conocido.

Por otra parte, muchos padres y profesores pertenecen aún a generaciones analógicas, enfrentándose con recelo y desconocimiento a las tecnología que en los últimos años lo han revolucionado todo. Es por eso que, en algunos medios, a estos niños nacidos en la era digital, cuyos padres no se han adaptado a ella, se les denomina, con cierta ironía, huérfanos digitales. Esta orfandad es una de las causas, entre otras muchas, de que en los colectivos más desfavorecidos se abra (o se amplié) una brecha digital, una grieta que separa a los bien adaptados tecnológicamente de los que no lo están, con las repercusiones para el futuro que eso puede suponer a nivel social, educativo o laboral.

Esta brecha digital se suple en muchos casos con la capacidad del niño nacido en una generación digital que, pese a todas las trabas que se le presenten, es capaz de saltar la grieta y adaptarse a las nuevas posibilidades. Sin embargo, en colectivos desfavorecidos (pobreza, marginación, discapacidad…) la brecha es más difícil de saltar, y el hecho de que sus padres o profesores sigan viviendo en su mundo analógico, no hace sino agrandarla.

Debemos hacer un esfuerzo por integrar a estos colectivos en este mundo tecnológico que avanza sin cesar y que amenaza con dejarlos infoexcluidos. Del mismo modo que educamos a nuestros hijos en el uso de diferentes tecnologías (teléfono, televisión, DVD…) o hábitos (cortesía, educación vial, medidas de seguridad, valores…) más arraigados en nuestra sociedad, Internet se ha convertido en uno de los pilares de la comunicación y la información hoy en día, y esto nos obliga a indicarles, desde pequeños, cuáles son las virtudes y los peligros de la red de redes, no solo porque es una herramienta imprescindible en su relación con el entorno social, sino porque constituye una potente herramienta de educación y relación padres-hijos.

Pero del mismo modo que en la vida real, la red también es un lugar donde el menor puede encontrar información no adecuada y, en ocasiones, se producen abusos.

Es por esto que aunque es normal que exista una lógica preocupación, no sería una actitud positiva mostrarse excesivamente restrictivo en su uso por parte de los menores, al contrario, se debe fomentar su uso de una manera segura.

BENEFICIOS

- Encontrar recursos educativos para su trabajo escolar: documentos, sonidos, fotografía , dibujos …, como en una enciclopedia inagotable
- · Aumentar sus capacidades de expresión oral, comprensión lectora y escritura, organización y evaluación de la información , etc.
- · Comunicarse en tiempo real con familia, amigos, etc.
- · Aprender a utilizar mejor las tecnologías digitales y mejorar las habilidades informativas, imprescindibles para la época en la que vivimos a nivel personal, educativo y para el mundo profesional.
- · Mejorar su autoaprendizaje
- · Desarrollar el sentido de la responsabilidad.
- · Mejorar la autoestima
- · Fomentar el pensamiento crítico
- · La páginas web les permite acceder a recursos educativos y culturales multimedia inaccesibles de otra manera, obtener información actualizada, y jugar a juegos divertidos y educativos, entre otras cosas.
- · El correo electrónico les permite comunicarse fácilmente y en cualquier momento con familiares y amigos, y enviar fotos, canciones y documentos.
- · Los chats les permiten relacionarse con otros niños y adultos, participar en canales específicos para menores y comunicarse instantáneamente con familiares, amigos, profesores, etc.
- · La mensajería instantánea les permite comunicarse, intercambiar archivos y trabajar colaborativamente.

- · Los blogs les permiten expresarse en el nuevo lenguaje multimedia, contactar con otros chicos y chicas con intereses comunes, y compartir opiniones.
- · Los juegos en línea les permiten divertirse, mejorar la coordinación visomanual, desarrollar la capacidad de respuesta y toma de decisiones, y poner a prueba sus capacidades.

RIESGOS

Seguimos a MARQUÉS al agrupar los riesgos de Internet en las siguientes categorías:

- **1. RIESGOS RELACIONADOS CON LA INFORMACIÓN (CON LOS CONTENIDOS)**

· ***Acceso a información poco fiable y falsa***. Existe mucha información errónea y poco actualizada en Internet, ya que cualquiera puede poner información en la red. Su utilización puede dar lugar a múltiples problemas: desde realizar mal un trabajo académico hasta arruinar una actuación empresarial.

· ***Dispersión, pérdida de tiempo***. A veces se pierde mucho tiempo para localizar la información que se necesita. Es fácil perderse navegando por el inmenso mar informativo de Internet lleno de atractivos "cantos de sirena". Al final el trabajo principal puede quedar sin hacer.

· ***Acceso de los niños a información inapropiada y nociva***. Existen webs que pese a contener información científica, pueden resultar inapropiadas y hasta nocivas (pueden afectar a su desarrollo cognitivo y afectivo) para niños y menores por el modo en el que se abordan los temas o la crudeza de las imágenes (sexo, violencia, drogas, determinados relatos históricos y obras literarias...). La multimedialidad de Internet puede hacer estos contenidos aún más explícitos e impactantes.

· ***Acceso a información peligrosa, inmoral, ilícita***. Existe información poco recomendable (pornografía infantil, violencia, todo tipo de sectas...) y hasta con contenidos considerados delictivos que incitan a la violencia, el racismo, la xenofobia, el terrorismo, la pedofilia, el consumo de drogas, participar en

ritos satánicos y en sectas ilegales, realizar actos delictivos... La globalidad de Internet y las diferentes culturas y legislaciones de los países hacen posible la existencia (por lo menos temporal, ya que grupos especiales de la policía dedicados a *delitos informáticos* realiza actuaciones a nivel internacional) de estas páginas web en el ciberespacio

- **2. RIESGOS RELACIONADOS CON LA COMUNICACIÓN INTERPERSONAL**

- ***Bloqueo del buzón de correo***. Hay personas que ignorando las normas de ***"netiquette"*** (pautas de comportamiento que facilitan la convivencia entre los usuarios y el buen funcionamiento de la red) adjuntan grandes archivos a los correos sin pedir previamente autorización al receptor del mensaje, con lo que acaban bloqueando temporalmente su buzón de correo.

- ***Recepción de "mensajes basura"***. Ante la carencia de una legislación adecuada, por e-mail se reciben muchos mensajes de propaganda no deseada (spam) que envían indiscriminadamente empresas de todo el mundo. En ocasiones su contenido es de naturaleza sexual o proponen oscuros negocios. Otras veces pueden contener archivos con virus.

- ***Recepción de mensajes personales ofensivos***. Al comunicarse en los foros virtuales, como los mensajes escritos (a menudo mal redactados y siempre privados del contacto visual y la interaccción inmediata con el emisor) se prestan más a malentendidos que pueden resultar ofensivos para algunos de sus

receptores, a veces se generan fuertes discusiones que incluyen insultos e incluso amenazas. Por otra parte, en ocasiones hay personas que son acosadas a través del e-mail con mensajes que atentan contra su intimidad.

- ***Pérdida de intimidad***. En ocasiones, hasta de manera inconsciente al participar en los foros, se puede proporcionar información personal, familiar o de terceras personas a gente desconocida. Y esto siempre supone un peligro. También es frecuente hacerlo a través de los formularios de algunas páginas web que proporcionan determinados servicios gratuitos (buzones de e-mail, alojamiento de páginas web, música y otros recursos digitales...)

- ***Acciones ilegales***. Proporcionar datos de terceras personas, difundir determinadas opiniones o contenidos, plagiar informaicón, insultar, difamar o amenazar a través de los canales comunicativos de Internet... puede acarrear responsabilidades judiciales (como también ocurre en el "mundo físico").

- ***Malas compañías***. Especialmente en los chats, MUDs.., se puede entrar en contacto con personas que utilizan identidades falsas con oscuras intenciones, en ocasiones psicópatas que buscan víctimas para actos violentos o delictivos a las que prometen estímulos, experiencias y amistad.

- **3. RIESGOS RELACIONADOS CON ACTIVIDADES CON REPERCUSIÓN ECONÓMICAS**

- ***Estafas***. En las compras y demás transacciones económicas (tiendas virtuales, bancos, servicios formativos...) que se realizan por Internet, especialmente si las empresas no son de

solvencia reconocida, la virtualidad muchas veces enmascara sutiles engaños y estafas a los compradores.

- ***Compras inducidas por una publicidad abusiva***. Aprovechando la escasa regulación de las actividades en Internet, las empresas utilizan sofisticados sistemas de marketing para seducir a los internautas e incitarles a la adquisición de sus productos, incluyendo publicidad subliminal. Sus anuncios de reclamo ("banners"...) aparecen en todo tipo de webs, y a veces resulta dificil separar los contenidos propios de la web de la publicidad. De manera que a veces se acaba haciendo compras innecesarias.

- ***Compras por menores sin autorización paterna***. Niños y jóvenes pueden realizar compras sin control familiar a través de Internet, en ocasiones incluso utilizando las tarjetas de crédito de familiares o conocidos.

- ***Robos***. Al facilitar información personal y los códigos secretos de las tarjetas de crédito por Internet, a veces son interceptados por ciberladrones y los utilizan para suplantar la personalidad de sus propietarios y realizar compras a su cargo. Con todo, se van desarrollando sistemas de seguridad (firmas electrónicas, certificados digitales...) que cada vez aseguran mas la confidencialidad al enviar los datos personales necesarios para realizar las transacciones económicas. Hay empresas que delinquen vendiendo los datos personales de sus clientes a otras empresas y estafadores.

- ***Actuaciones delictivas por violación de la propiedad intelectual***. Muchas personas, a veces incluso sin ser conscientes de ello o de la gravedad de su acción, realizan actos delictivos violando la propiedad intelectual a través de Internet: búsqueda y recepción de programas o música con copyright (piratería musical) o software para desactivar sistemas de protección de los porductos digitales, difusión de estos materiales a personas conocidas...

- ***Realización de negocios ilegales*** a través de Internet: compra-ventas, subastas, préstamos, apuestas...

- ***Gastos telefónicos desorbitados***. Si no se dispone de una conexión adecuada con tarifa plana que fije el coste mensual por uso de Internet, o el internauta entra de manera inconsciente en páginas (generalmente de contenido sexual) en las que al solicitar un servicio aparentemente gratuito le conectan a líneas telefónicas de alta tarifación, las facturas telefónicas pueden proporcionar serios disgustos.

- **4. RIESGOS RELACIONADOS CON EL FUNCIONAMIENTO DE INTERNET**

- ***Lentitud de accesos***. A veces debido al tipo de conexión (modem...), otras veces debido a la saturación de algunos servidores en horas punta.

- ***Imposibilidad de conexión a una web o a un servicio de Internet***, que puede ser dedida a problemas del servidor que da el servicio. Si esta circunstancia nos impide la realización de un trabajo importante, puede traernos muy malas consecuencias.

- ***Problemas de virus***, que actualmente se propagan con libertad por la red y pueden bloquear el funcionamiento del ordenador y destruir la información que almacena. Para navegar por Internet resulta imprescindible disponer de un sistema antivirus actualizado en el ordenador.

- ***Espionaje***. A través de mecanismos como las "cookies" o de virus, se puede conocer todo lo que se hace desde un ordenador y copiar todos los archivos que tiene amacenados. Con estos sistemas algunos espías se dedican a detectar las circunstancias y preferencias de las personas con el fin de elaborar listas de posibles clientes que luego venden a las empresas comerciales.

- ***Publicidad subliminal, spam...***

- **5. RIESGOS RELACIONADOS CON LAS ADICCIONES**

Podemos considerar que una persona tiene **adicción a Internet** (IAD, Internet Addiction Disorder) cuando de manera habitual es **incapaz de controlar el tiempo que está conectado a Internet**, relegando las obligaciones familiares, sociales y académicas/profesionales. Muchas veces además roban horas al sueño e incluso se reduce el tiempo de las comidas; de manera que el cansancio y la irritabilidad se irán cronificando, así como la debilidad del sistema inmunológico y muchas veces una cierta tendencia al aislamiento social.

Más que una adicción genérica a Internet, podemos considerar adicciones o usos compulsivos a determinados contenidos o servicios:

- ***Adicción a buscar información*** de todo tipo: noticias, webs temáticas, webs personales, servicios ofrecidos por empresas... Muchas veces incluye pornografía, imágenes o escenas que incluyen violencia... Se buscan sensaciones más que información.

- ***Adicción a frecuentar los entornos sociales***: chats, MUDs... Los usuarios no dependientes tienen más tendencia a comunicarse con las personas conocidas. Los adictos buscan más conocer gente nueva y buscar el apoyo en los grupos de la red; a veces se crean varias personalidades virtuales.

- ***Juego compulsivo***. Internet está lleno de webs con todo tipo de juegos, algunos de ellos tipo casino con apuestas en dinero;

otros muy competitivos o violentos..., que pueden fomentar ludopatías en determinadas personas.

- ***Compras compulsivas:*** comercio electrónico, subastas...

RIESGOS ESPECÍFICOS EN CADA SERVICIO DE INTERNET

(Tomado de Internetsegura.net)

WEBS

Básicamente hay dos posibles riesgos asociados con la visita de páginas web. En primer lugar, un niño puede encontrarse con contenidos ilegales o nocivos. En segundo lugar, algunas webs invitan a los visitantes a dar información sobre ellos mismos. Por eso, antes de dar información personal, sería conveniente que los niños lo hablaran con la familia. Consultar la política de privacidad de la web es muy recomendable para estar más seguros del uso que harán de los datos.

BLOGS

Los niños y adolescentes pueden construir sus propios blogs (gratuitamente), actividad que puede ser muy educativa y beneficiosa. Pero hace falta ir con cuidado, porque todo lo que se cuelga en Internet queda a la vista de cualquier visitante. Si los chicos tienen un blog, una medida de prevención sería visitarlo a menudo para ver qué publican, garantizando que no haya datos que puedan identificarlos (el nombre y apellido, la dirección, el teléfono o una fotografía). También podéis supervisar que no se presenta información que pueda ser nociva u ofensiva para otra gente, ni que pueda exponer a los menores y adolescentes a problemas en la escuela o incluso a nivel legal.

CHAT

El chat es una actividad muy popular entre la gente joven, especialmente los adolescentes, porque les permite comunicarse con gente de todas partes y hacer nuevos amigos y amigas.

Pero también es una de las áreas dónde se pueden poner en situación de riesgo con más facilidad, especialmente por tres motivos:

- fácilmente pueden olvidar que se trata de un lugar público;

- no necesariamente conocen la verdadera identidad de los otros participantes;

- la mayoría de chats no están moderados, es decir, no hay nadie que los controle.

Es habitual entre los adolescentes “conocer” a alguien en un canal de chat que se gana su confianza siendo simpático y queriendo "escuchar" sus problemas. Por eso los niños y especialmente los adolescentes deberían tener mucho cuidado en no revelar nunca su identidad y no creerse todo lo que les diga la gente.

Si quieren quedar con una persona que han conocido a través del chat, sería conveniente que antes hablaran con la familia. Si estos estuvieran de acuerdo con el encuentro, sería más seguro que algún adulto los acompañara, y que la cita tuviera lugar en un espacio público.

MENSAJERÍA INSTANTÁNEA

El envío de "mensajes instantáneos" permite a la gente establecer conversaciones de texto a tiempo real directamente con otras personas de nuestra “lista de contactos”.

El software también permite intercambiar archivos y activar nuestra webcam para establecer contacto visual con nuestros amigos e incluso, establecer conversaciones orales.

Se puede decir que es como un chat, excepto que normalmente es una experiencia sólo entre dos personas, en lugar de ser una actividad en grupo. De alguna manera es más seguro que un chat dado que podemos controlar nuestra lista de contactos reduciéndola a nuestros amigos o parientes.

Pero si se tratara de un desconocido podría llegar a ser más arriesgado. A diferencia de los chats, no hay nunca nadie más que pueda controlar o moderar la actividad y, por lo tanto, cuando vuestros hijos o alumnos participan en un envío de mensajes instantáneos con otros, es como si estuvieran solos en una sala privada. Controlar la lista de contactos es la mejor medida por evitar riesgos.

CORREO ELECTRÓNICO

A veces nuestros menores reciben mensajes de personas desconocidas. Esto puede resultar arriesgado especialmente en dos casos:

a) Cuando se trata de mensajes comerciales no deseados (mensajes de correo basura).

b) Cuando se trata de alguna persona que intenta inducir al menor a establecer una relación inadecuada o lo amenaza.

Si se diera el caso y sospecharais que los menores pudieran estar en riesgo, lo más conveniente sería poneros en contacto con la policía.

Algunos **instrumentos de control**, os pueden ayudar a bloquear el correo basura o los mensajes enviados por personas concretas.

FOROS

Los foros o grupos de discusión son áreas de Internet en las que la gente puede intercambiar ideas, recetas, hechos, historias, fotos, o cualquier otra cosa. Hay miles de grupos de discusión sobre toda clase de temas: música, deportes, profesiones, escuelas... cualquier cosa. La mayoría de los grupos de discusión son correctos, pero hay algunos que no son adecuados para los niños.

Para prevenir posibles situaciones de riesgo, hay varios **instrumentos de control** que os pueden ayudar a impedir que el niño tenga acceso a ciertos tipos de grupos de discusión. También es importante que los niños aprendan que no se debe responder mal en los grupos de discusión. Hace falta ser respetuosos y no ofender a nadie.

CONSEJOS

- · Es necesario que los padres aprendan a utilizar el ordenador. De este modo y hasta cierta edad, se conectan con ellos y el niño aprende a disfrutar de Internet junto a sus padres; además conocer el ordenador ayuda a los padres a distinguir qué software utiliza y qué páginas visita el menor más fácilmente.
- · Disfrutar de Internet con sus hijos e hijas.
- · Fomentar el diálogo sobre hábitos de navegación y sus riesgos. Es importante que el menor sienta que cuando le suceda algo extraño para él o que le incomode pueda decírselo a sus padres sin sentirse culpable. Además les ayudaremos a mantener un espíritu crítico sobre la información que aparece en la red y les explicaremos que no todas las webs tienen la misma credibilidad. Hablar siempre con los hijos sobre lo que hace y encuentra en Internet.
- · Acordar unas normas de uso claras. Es particularmente bueno que los niños tengan reglas claras sobre lo que pueden o no hacer y conocer sus consecuencias, especialmente respecto al tiempo de uso (de día y

no de noche, controlar su uso entre semana), de esta manera el niño sabrá a priori a lo que atenerse.

- · Es necesario colocar el ordenador en una zona de uso común. Facilitará la supervisión tanto del tiempo de uso (para controlar la ciberadicción) como el control de situaciones que puedan incomodarle, como por ejemplo, para evitar el ciberacoso cuando utilizan la webcam.
- · Enseñarles en qué consiste la privacidad. Explicarles que los datos personales son información sensible y que puede ser utilizada en su contra con ejemplos de la vida cotidiana, como puede ser, por ejemplo, que ellos nunca darían las llaves de casa a un desconocido o ejemplos similares.
- · Explicarles que en la red también hay que respetar a los demás. Que entiendan que detrás de un apodo, hay personas y que también hay que ser cortés y educado con ellas.
- · No culpabilice a sus hijos e hijas sobre lo que ocurra en Internet, ni sea alarmista.
- · Tener un cortafuegos (firewall) y un antivirus actualizado que proteja el ordenador de los virus y de los programas espía.
- · Utilizar navegadores infantiles (que solo acceden a páginas adecuadas) o instalar programas protectores que filtren la información facilitando el acceso a sitios web seguros y controlando el tiempo de conexión.
- · Es una buena ayuda utilizar filtros de control de acceso a la red. Así evitará que acceda a paginas de contenido inapropiado (adulto, violento, xenófobo, etc.). En el mercado existen soluciones gratuitas y muchos proveedores ofrecen soluciones de este tipo.
- · Si se detecta algún peligro, contactar con las autoridades o con instituciones como "Protégeles"
- · Conviene que los padres hablen con los centros educativos para asesorarse y conocer cómo se trata el tema en la escuela.

CONSEJOS PARA NIÑOS HASTA 10 AÑOS

- · Nunca es demasiado pronto para fomentar una comunicación abierta y positiva con sus hijos. Es recomendable hablar con ellos acerca de los equipos y estar abierto a sus preguntas y a su curiosidad.
- · Siéntese junto a sus hijos de esta edad cuando se conecten a Internet.
- · Establezca reglas claras para el uso de Internet.
- · Insista a su hijo para que no comparta información personal, como su nombre real, dirección, número de teléfono o contraseñas con las personas que conozcan por Internet.
- · Si desde un sitio se anima a los niños a que envíen sus nombres para personalizar el contenido web, ayúdeles a crear alias que no revelen información personal cuando estén en línea.
- · Infórmese acerca de las herramientas de filtrado web para ayudarle a implicarse con sus hijos y en la supervisión de los padres.
- · Al usar herramientas de seguridad familiar, cree perfiles apropiados para cada miembro de la familia en función de su edad.
- · Contribuya a proteger a sus hijos de ventanas emergentes ofensivas mediante un bloqueador de elementos emergentes.
- · Todos los miembros de la familia deben actuar como modelos para los niños que empiecen a usar Internet.
- · Conocer las claves de acceso. Ayudarles a escoger unas buenas claves de uso y explicarles la razón de esto.

CONSEJOS PARA NIÑOS DE 11 A 14 AÑOS

.

- Es recomendable fomentar una comunicación abierta y positiva con los hijos. Hable con ellos acerca de los PC y muéstrese abierto ante sus preguntas y su curiosidad.
- · Establezca reglas claras para el uso de Internet.

- · Insista a su hijo para que no comparta información personal, como su nombre real, dirección, número de teléfono o contraseñas con las personas que conozcan por Internet.
- · Si desde un sitio se anima a los niños a que envíen sus nombres para personalizar el contenido web, ayúdeles a crear alias que no revelen información personal cuando estén en línea.
- · Use herramientas de protección infantil que le permitan crear perfiles adecuados para cada miembro de la familia.
- · Establezca las herramientas de protección infantil en una configuración de seguridad de nivel medio, de forma que haya limitaciones en el contenido, en los sitios web y en las actividades.
- · Mantenga los equipos conectados a Internet en un área abierta en que pueda supervisar fácilmente las actividades de sus hijos.
- · Investigue herramientas de filtrado de Internet como complemento a la supervisión parental.
- · Contribuya a proteger a sus hijos de ventanas emergentes ofensivas mediante un bloqueador de elementos emergentes.
- · Invite a sus hijos a que le digan si alguien o algo de Internet les hace sentir incómodos o amenazados. Conserve la calma y recuerde a sus hijos que no se meterán en problemas por llamar su atención acerca de algo. Felicíteles por su comportamiento y anímeles a que recurran a usted si se repite la situación.
- · Enseñar los chavales a no descargar nada sin permiso: Muchas veces tienen la falsa creencia de que el nombre del archivo es indicativo del programa que están descargando, o en ocasiones descargan algo en el ordenador sin saber muy bien por qué lo han hecho.

CONSEJOS PARA ADOLESCENTES DE 15 A 18 AÑOS

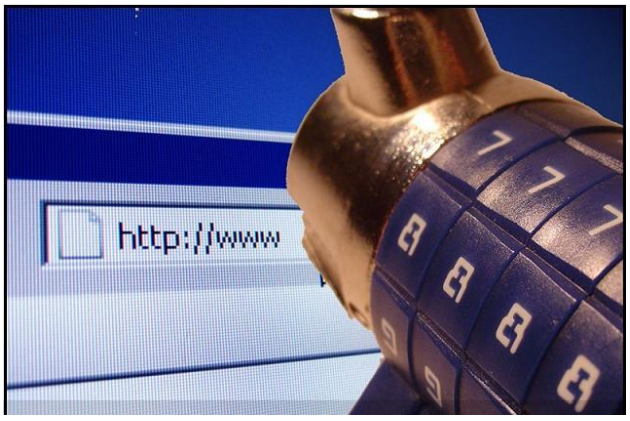
- · Asegúrese de que la comunicación familiar acerca del uso de los equipos sea lo más abierta y positiva posible. Continúe hablando acerca

de sus experiencias, amistades y actividades en línea, del mismo modo que en el caso de las demás actividades y los amigos que conocen por otros medios.

- También debe invitar a sus hijos a que le digan si algo o alguien les hace sentir incómodos o amenazados cuando exploran, juegan o se comunican a través de Internet. Si es adolescente y encuentra algo o a alguien en línea que no parezca correcto, comuníquelo.
- · Elabore una lista de reglas de Internet en casa como familia. Incluya qué tipo de sitios está fuera de los límites, las horas a las que se pueden conectar, qué tipo de información no deben compartir en línea e instrucciones para comunicarse con otras personas en línea, incluidos los salones de chat.
- · Conserve los equipos con conexión a Internet en una zona abierta y no en los dormitorios de sus hijos.
- · Investigue herramientas de filtrado de Internet como complemento a la supervisión parental.
- · Contribuya a proteger a sus hijos de ventanas emergentes ofensivas mediante un bloqueador de elementos emergentes.
- · Sepa qué salones de chat o paneles de mensajes visitan sus hijos adolescentes, y con quién hablan. Anímeles a usar salones de chat con moderador e insista en que permanezcan en las áreas públicas de esos salones.
- · Insista en que nunca acepten encontrarse con alguien a quien hayan conocido a través de Internet.
- · Enseñe a sus hijos que no deben descargar programas, música ni archivos sin su permiso. Compartir archivos y tomar texto, imágenes o material gráfico de la Web son acciones que pueden suponer una infracción de las leyes de copyright y ser ilegales.
- · Hable con sus hijos adolescentes acerca del contenido adulto y la pornografía en línea, y diríjalos a sitios positivos acerca de la salud y la sexualidad.
- · Ayúdeles a protegerse del correo no deseado. Indique a sus hijos adolescentes que no faciliten su dirección de correo electrónico en línea, que no respondan al correo no deseado y que usen filtros de correo electrónico.
- · Esté atento a los sitios web que visitan sus hijos adolescentes. Asegúrese de que sus chicos no visitan sitios con contenido ofensivo, ni que publican información personal ni fotografías propias.
- · Eduque a sus hijos acerca de las conductas éticas y responsables en Internet. No deben usar Internet para difundir rumores, intimidar ni amenazar a nadie.
- · Asegúrese de que sus hijos adolescentes le consultan antes de realizar transacciones financieras en línea, tales como realizar pedidos o compras o vender artículos.
- · Hable con sus hijos adolescentes sobre los juegos de azar en línea y sus riesgos potenciales. Recuérdeles que no pueden jugar dinero en línea, ya que es ilegal.

- · Conocer los remitentes para no tener que leer los correos. A partir de la preadolescencia, los jóvenes son muy celosos de su privacidad, entonces se puede establecer un acuerdo intermedio en el que los padres conozcan las direcciones, al igual que el correo postal, pero no lean el correo electrónico -en el correo postal se puede leer el remitente, pero no es necesario abrir la carta-, y en el caso de que exista una dirección desconocida, es mejor preguntar al menor.
- · Muéstrese interesado por las amistades que sus hijos e hijas hacen online, especialmente en los sistemas de «Chats» y de mensajería instantánea.
- · Enseñarles a tener un comportamiento responsable, respetuoso y ético en Internet. En muchas ocasiones tienen una falsa sensación de impunidad, que les hace atreverse con actitudes más agresivas, que en la vida real jamás adoptarían. Por esto, es recomendable explicarles que, cuestiones como el ciberacoso no puede ser divertido cuando se le hace daño o se molesta al prójimo.

HERRAMIENTAS DE CONTROL



- · **Herramientas que bloquean contenidos**

Los denominados **"filtros"** son programas que bloquean el acceso a contenidos considerados ilegales o nocivos (ya sean palabras, imágenes, películas, sonidos).

Podemos encontrar diferentes sistemas:

- **Direcciones web (URL)**: limita el acceso a una lista específica de webs que se han considerado inadecuadas (lista de páginas negativas). Con este sistema se bloquean las páginas teniendo en cuenta el texto, el contexto, las imágenes, etc., y se puede trabajar a la vez con tantos idiomas como se quiera.

  En las listas negativas se incluyen todas las páginas que se consideran nocivas. Pero cada día se crean centenares de páginas web, y para el productor del programa es prácticamente imposible revisarlas e incluirlas en sus listas instantáneamente. Hay demasiada cantidad de documentos; el margen de error es demasiado grande y las listas quedan obsoletas tan pronto como aparecen.

  De ahí que algunos fabricantes hayan optado por ofrecer listas de páginas positivas, con claros contenidos apropiados. Cuando el niño acceda a Internet, sólo podrá visualizar a las páginas que estén incluidas en la lista.

  Según los expertos, el uso de listas positivas es por ahora la modalidad más segura. A menudo a una herramienta de prevención que sólo utiliza listas positivas se le denomina "navegador infantil" (walled garden), porque ofrece un conjunto de webs por las cuales el menor puede navegar tranquilo, es decir, una área dentro de Internet donde, en principio, se puede mover con seguridad.

  Otra opción de selección pueden ser los sellos de calidad, como el sello de IQUA. Este tipo de certificación de las páginas nos garantizan la adecuación de sus contenidos para los menores y adolescentes.

- **Bloqueo de palabras clave**: limita el acceso a una lista específica de palabras que pueden ser "inapropiadas", como por ejemplo "sexo", "pecho". Algunas herramientas sólo bloquean las palabras, pero no todo el texto en el que aparecen. Según la herramienta, pueden trabajar en diferentes servicios por separado o a la vez: páginas web, correo electrónico, tertulias, mensajería instantánea, foros, etc.

  La herramienta puede funcionar en uno o más idiomas. Un inconveniente es que ciertas páginas web específicas de adultos han aprendido a saltarse estos bloqueos, escribiendo palabras mal (añadiendo una k, por ejemplo, al final de la palabra) para que la herramienta no las detecte.

- **Bloqueo de palabras clave en su contexto**: para evitar que no se bloqueen por error contenidos que, por ejemplo, traten sobre la prevención del uso de drogas, el cáncer de mama, etc., la herramienta puede analizar cada palabra en su contexto.

- **Bloqueo de imágenes**: algunas herramientas llegan a bloquear imágenes "nocivas", como por ejemplo fotografías de pornografía infantil, de violencia extrema, etc.

- **Etiquetado y clasificación de contenidos**: la clasificación de un contenido consiste en asignar a cada documento o lugar de Internet un conjunto de etiquetas (PICS, Platform for Internet Content Selection) que definen el tipo de información mostrada. Por ejemplo, etiquetamos una película como "Todos los públicos" o "Para mayores de 18". Sería el equivalente a poner los "rombos" (etiquetas) de las películas (contenidos) y además poder decirle al televisor (navegador) si queremos ver o no las películas con rombos.

  Los creadores/editores de páginas web pueden autoetiquetar sus documentos, como lo hacen los fabricantes de juguetes. Con este sistema de etiquetado de contenidos es muy fácil aplicar "filtros" y también en navegadores y motores de búsqueda. El asesor de contenidos del navegador Internet Explorer, por ejemplo, lo trae incorporado.

- Una alternativa al etiquetado, con más ventajas y prestaciones, es el **sistema RDF** (Resource Description Framework – Infraestructura para la Descripción de Recursos). Es un vocabulario de XML (lenguaje informático de etiquetado) que está destinado a convertirse en el estándar universal para la definición y la búsqueda de metadatos (datos que nos permiten localizar otros datos, por ejemplo la referencia bibliográfica de un libro en la base de datos de una biblioteca).

  Gracias al RDF podremos descubrir y encontrar recursos en la red más fácilmente a través de los motores de búsqueda y conseguiremos una navegación más rápida y eficiente.

- · **Herramientas que limitan el tiempo de conexión**

Programas útiles para las familias que estén preocupadas porque los niños se pasan muchas horas en Internet. También puede interesar en los casos en que pasan mucho tiempo solos en casa. Puede ayudar a establecer lo siguiente:

¿Cuántas horas al día nuestros niños navegan por Internet?

¿Cuántos días a la semana?

¿Cuánto tiempo han tenido puesto en marcha el ordenador?

- · **Navegadores infantiles**

Herramientas que dan acceso a páginas adecuadas para los niños y adolescentes. Tienen un diseño y características apropiadas a este público. Permiten el uso de diferentes perfiles, en función de la edad del usuario.

- · **Buscadores infantiles**

Buscadores, gratuitos, dirigidos a los niños y adolescentes, que buscan contenidos adecuados para su edad.

- · **Herramientas que registran los lugares web visitados**

Estos programas permiten el acceso a todos los contenidos de Internet, pero informan y facilitan el seguimiento de las páginas web que visitan los niños. Estas herramientas guardan en la memoria del ordenador los nombres de los lugares web que visita, para que las familias o educadores los puedan supervisar más tarde.

- · **Herramientas que bloquean la entrada de mensajes de correo "basura"**

Programas que bloquean información que "entra" en el ordenador a través del correo electrónico (mensajes recibidos desde direcciones determinadas, mensajes "basura" (spam), mensajes con lenguaje ofensivo, etc.).

- · **Herramientas que bloquean la información que sale del ordenador**

Estos programas impiden revelar información personal, como por ejemplo el número de teléfono, la dirección, el número de tarjeta de crédito u otras señas personales. Esto es especialmente interesante con respecto a llenar formularios y hojas de registro en línea, comprar a través de la tarjeta de crédito, etc. y, si llegaran a hacerlo, en la pantalla aparecería XXX en lugar de sus datos reales. Puede ser utilizado tanto para la red, como para el correo electrónico, como para los chats, etc.

- · **Herramientas que permiten regular el uso de los servicios de Internet**

Programas que determinan qué servicios de Internet puede utilizar cada usuario (tertulias, correo electrónico, consulta de páginas web, etc.), en función de los criterios de cada familia. Se puede permitir, por ejemplo, sólo el uso de chats determinados, que estén moderados.

NAVEGADORES INFANTILES

Se trata de herramientas muy útiles que permiten solo el acceso a aquellos sitios de Internet que hemos seleccionado previamente.

Suelen tener un aspecto infantil y ser muy sencillos de usar por el niño, aunque tienen un módulo de configuración muy completo para los padres.

Tienen funciones como la de limitar el tiempo de uso, bloquear la pantalla para no poder usar más que el navegador, cambiar los fondos, usar un correo

electrónico infantil con entradas y salidas restringidas, historial, favoritos, etc.

Aunque muchos están en inglés, los hay que admiten varios idiomas, e incluso alguno está desarrollado en español.

BUDDY BROWSER

Muy atractivo pero solo en inglés.

http://www.buddybrowser.com/

# # #

KIDO´Z

Atractivo y sencillo de usar… y en español.

http://kidoz.net/index.html

# # #

KIDZUI

Muy completo, pero en inglés.

http://www.kidzui.com/

# # #

PIKLUK

En inglés, pero tan sencillo de usar que no importa.

http://www.pikluk.com/

# # #

KID ROCKET

Otro buscador infantil en inglés.

http://kidrocket.org/

NAUTILUS

Buscador en español.

http://www.navegadornautilus.com/

Descarga en: Taringa

# # #

ZAC BROWSER

Originalmente para autistas, pero excelente para todos. En español.

http://www.zacbrowser.com/es/

BUSCADORES INFANTILES

Se trata de buscadores de Internet que restringen los resultados de la búsqueda según distintos criterios. Además de los criterios que por defecto usa cada buscador, se pueden personalizar.

De esta manera, cuando el niño realiza una búsqueda en Internet, solo obtiene como resultados páginas infantiles u otras cuyos contenidos están libres de violencia, sexo, drogas, racismo, xenofobia, terrorismo, pedofilia u otros contenidos nocivos, peligrosos o ilícitos.

BUSCADOR INFANTIL

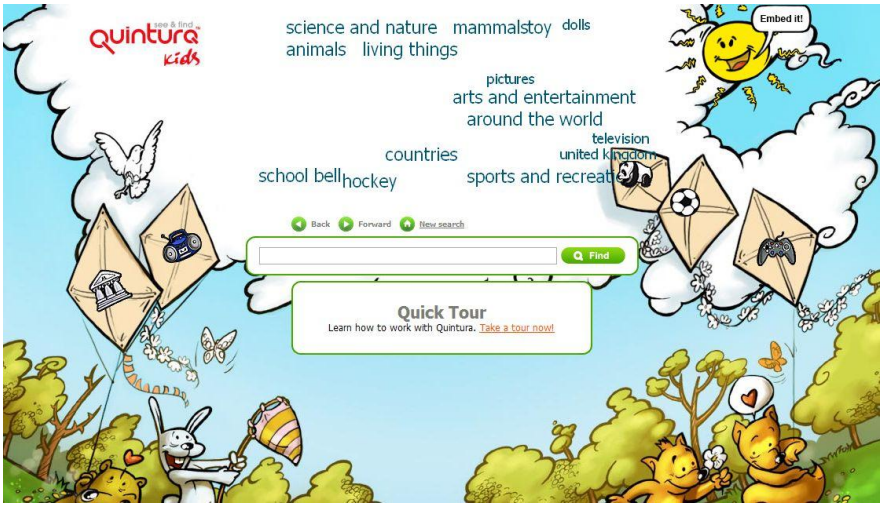
Búsquedas potentes de calidad. En español.

http://www.buscadorinfantil.com/index.html

QUINTURA KIDS

Buscador y directorio. En inglés.

http://quinturakids.com/



ABCHICOS

Buscador y directorio muy completo. En español.

http://www.abchicos.com.ar/abchicos/

CURIOSOS.COM

Buen buscador y directorio en español, aunque demasiado sobrio.

http://curiosos.com/

# # #

ASK KIDS

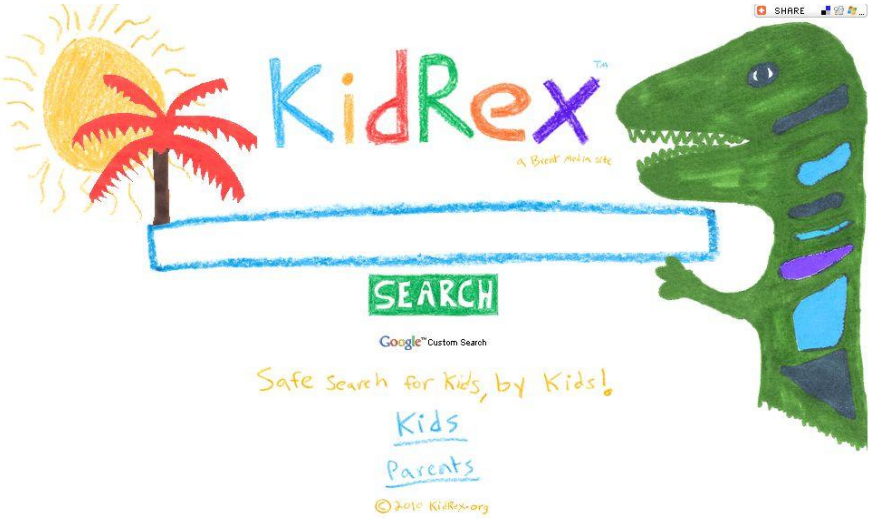
Buen buscador en inglés.

http://www.askkids.com/

KIDREX

Buscador infantil en inglés.

http://www.kidrex.org/



FILTROS DE CONTROL PARENTAL

Existen muchas herramientas para el control parental con filtros que bloquean contenidos, palabras clave, direcciones, imágenes o etiquetas; que bloquean el tiempo de conexión; que guardan las páginas visitadas para luego poder verlas los padres; que bloquean la entrada de correo basura o la salida de datos personales; que limita el tipo de servicios de Internet a los que se puede acceder, etc.

En algunos casos son gratuitos y en otros son de pago, y aunque nunca pueden ser efectivos al 100%, resultan buenas herramientas de seguridad para los niños.

WINDOWS LIVE PROTECCIÓN INFANTIL

http://explore.live.com/windows-live-family-safety

Es un servicio de la empresa Microsoft.

Es un servicio gratuito integrado en Windows Live que permite configurar varias cuentas con distintos niveles de protección, personalizando la configuración de cada una, y recibiendo informes distintos. Realiza un filtrado web y da informes detallados de las páginas que se han visitado (o intentado visitar), los programas usados y el tiempo empleado. Administra los contactos para decidir con quién se puede hablar a través de Windows Live Spaces, Messenger y Hotmail.

CONTROL PARENTAL AMIGO

http://www.amigoweb.es/

Es un producto de la empresa Aconfi S.L.

Permite guardar un historial detallado de los sitios visitados, así como un historial de pantallas de esos sitios. Se pueden limitar aplicaciones y contenidos. No es detectable y se lanza por combinación de teclas.

Su precio es de 68€.

CANGURO NET y CANGURO NET PLUS

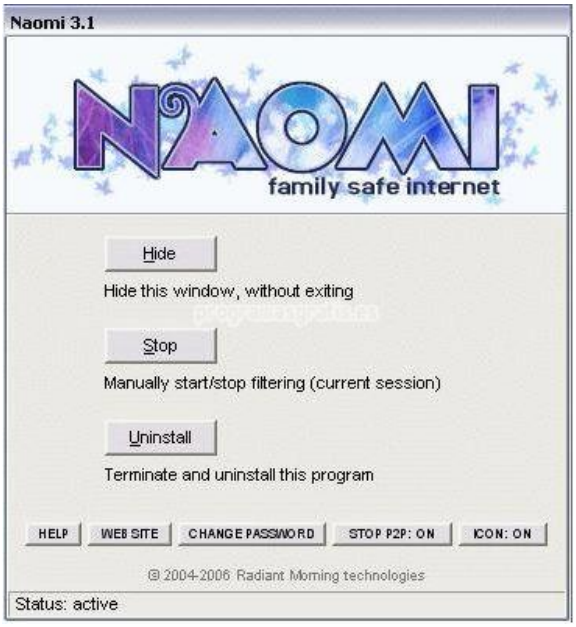
http://www.movistar.es/

Es un servicio de Telefónica de filtrado de contenidos y publicidad de Internet que permite a los clientes de Telefónica con una conexión ADSL, bloquear el acceso a determinadas páginas web y la descarga de determinados archivos. Al ser un servicio proporcionado por el proveedor de acceso a Internet, no requiere ninguna instalación de software en nuestro ordenador. Esto permite que el mantenimiento y las actualizaciones se realicen automáticamente sin ninguna molestia para el usuario.

Hay que pagar una cuota de 2,60 o 3,50 €. (año 2010)

NAOMI

Descarga en http://naomi.programasgratis.es/



Naomi es un programa que viene a filtrar semántica y heurísticamente las webs en las que se entra desde tu ordenador, con el fin de que los más pequeños no entren en determinadas páginas.

El comportamiento de Naomi ante esta situación es muy simple, desactiva el navegador con lo que tus hijos no van a llegar ni a ver lo que aparezca en la pantalla, y tampoco van a poder hacer correcciones en la configuración del programa, porque está gestionado con contraseñas, para una mayor seguridad.

Gratuito.

CYBER PATROL

http://www.cyberpatrol.com/cpparentalcontrols.asp

Es un producto de la empresa Surf Control.

Filtro disponible tanto a nivel de usuario como de servidor. Filtra aproximadamente un millón de webs en 12 categorías, incluyendo desnudez, alcohol, juegos de azar, odio y violencia. El usuario/a puede escoger qué categorías filtrar a partir de una lista. Cyber Patrol permite determinar hasta 10 perfiles diferentes de usuarios. Además del filtro, incorpora la opción de restringir el número de horas de conexión a Internet. Sólo disponible en inglés.

Software a partir de 40 € para 3 PCs. (año 2010)

# # #

NYS BLOCK CONTROL PARENTAL

Descarga en: http://nysblock-control-parental.programasgratis.es/

Utiliza esta herramienta gratis, y podrás controlar lo que hacen tus hijos, así como también limitar el tiempo que están ante del PC. Entre las características que presenta nysBlock Control Parental, encontrarás la posibilidad de bloquear aplicaciones (incluyendo juegos y servicios de mensajería instantánea), en un horario determinado. Y en el caso de que se intente acceder a ellas, se enviará un correo electrónico a los padres para que ellos decidan qué hacer.

NysBlock Control Parental está en español, de manera que resultará mucho más sencillo configurar el programa.

Gratuito.

NET NANNY

http://www.netnanny.com/

Es un producto de la empresa BioNet Systems.

Net Nanny
POWERED BY [content]watch.

Herramienta que incluye una base de datos de páginas web en español e inglés, censuradas por su contenido pornográfico. También ofrece otras opciones como por ejemplo el filtrado del correo entrante y saliente para verificar que no contenga palabras inapropiadas, bloqueo de publicidad, control de tiempo de conexión, bloqueo de acceso a programas de Internet considerados inadecuados (mensajería electrónica, juegos en línea...) y bloquea y graba las sesiones de chat. Es una de las herramientas más utilizadas y completas también disponible en versión en español.

Software entre 40 y 50 € (año 2010).

# # #

OPTENET

http://www.optenet.es/es/home.asp

Producto de la empresa Optenet.

Filtro de selección de contenidos para ámbitos domésticos, educativos y laborales, de fácil instalación. Funciona a nivel de usuario y a nivel de servidor. Dispone del motor de análisis de páginas web más potente del mercado, así como listas de protección predefinidas y un sistema de personalización, que permite añadir o sacar direcciones de manera rápida. También permite filtrar la descarga de artículos, determinar horarios de navegación según perfiles de usuario y ver el histórico de navegación de cada usuario. Está disponible en español, inglés, francés e italiano.

Software con un precio de 40€ (año 2010)

# # #

CYBER SITTER

http://www.cybersitter.com/

Producto de la empresa Solid Oak Software, Inc.

Filtro fácil de utilizar que bloquea 10 categorías de contenido. Los educadores y educadoras pueden personalizar los contenidos filtrados, añadiendo webs que consideren nocivas o eliminando alguna de las categorías. Las actualizaciones son automáticas una vez por semana, pero también pueden hacerse manualmente cuando se quiera. Además del filtro, se incorporan las opciones de grabar las webs visitadas por el menor y de bloquear información que entra o sale (preguntas, datos personales, palabras nocivas). Sólo disponible en inglés.

Soluciones a partir de 30 € (año 2010)

# # #

CYBER SNOOP

http://www.pearlsw.com/index.asp

Es un producto de la empresa Pearl Software, Inc.

Analizador que nos permite saber lo que hacen los menores en Internet, con respecto a visitar webs, participar en foros, chats, guardar o enviar archivos

(FTP) y utilizar el correo electrónico. Por ejemplo, podemos saber cuánto tiempo pasan en Internet e impedir el envío de datos personales. También se incorpora un filtro de acceso a contenidos que podemos utilizar tanto a nivel de usuario como de servidor. Se filtran categorías como sexo, violencia, odio, actividades ilegales, entre otras. Podemos acceder a los criterios utilizados por la empresa y variarlos. También podemos acceder a las listas de webs filtradas y personalizarlas añadiendo o sacando webs.

# # #

ONLINE FAMILY NORTON

https://onlinefamily.norton.com/familysafety/whyUseNOF.fs

Es un producto de la empresa Symantec.

Es un sistema de control parental con el cual se puede ayudar a asegurar la navegación de los niños en la red. Pero esta solución no solo se centra en el navegador, sino también en diversos aspectos de la vida social online, por ejemplo su participación en redes sociales o clientes de mensajería instantánea. En español y gratuito.