Guía parental

Manteniendo a sus niños seguros en Internet

protegeles.com

ins@fe

Apoyado por:

chellomulticanal
a Chellomedia company

RESUMEN

A. Cómo utilizar este kit

Si planeas a un año, planta arroz.
Si planeas a diez años, planta un árbol.
Si planeas por una vida, educa a tus hijos.

Proverbio chino

Estimado Padre/Tutor,

Usted está frente al kit de seguridad informática para familias con niños de entre 6 y 12 años. Es un recurso educativo creado en base a la firme creencia de que las nuevas tecnologías no deberían separar a las generaciones sino unirlas. Ha sido creado gracias a la experiencia de Insafe, la red paneuropea de nodos nacionales de sensibilización sobre un uso seguro de nuevas tecnologías por parte de los menores, en el caso de España, la asociación PROTEGELES, que trabajan para aumentar la concienciación de la población acerca de los problemas de seguridad vinculados a Internet. El desarrollo y la producción de este kit de seguridad informática fueron apoyados por UPC.

Así como jugar en un patio de recreo o cruzar la calle puede resultar peligroso si no está atento, el uso de Internet y de las tecnologías de la información y la comunicación también implica peligros para alguien imprudente. Afortunadamente, existen recursos que permiten a los usuarios de Internet tener conocimiento acerca de los beneficios y los riesgos de navegar por la Web.

Utilice su nuevo kit para apoyar a sus hijos en el aprendizaje de cómo utilizar Internet con seguridad y eficiencia. El kit ofrece más de cincuenta consejos de seguridad y ejercicios para ayudarle a enseñar seguridad informática a sus hijos de un modo divertido, atractivo y no amenazante. Incluye:

- Dos cuadernillos de seguridad informática: una sección de diversión familiar y una guía para los padres;
- Reglas de oro;
- Un certificado familiar;
- Un conjunto de pegatinas;
- 12 tarjetas de situación para recortar;

Tanto el cuadernillo para padres como el familiar utilizan un código de colores para indicar cuatro temas de seguridad informática claves: La prevención brinda seguridad, Comunicación, Acoso en la red y Entretenimiento y descargas. El cuadernillo para padres sirve como referencia para la sección de diversión familiar: contiene información de fondo, notas sobre las actividades, y soluciones propuestas a los ejercicios y a las tarjetas de situación.

El cuadernillo para la familia está pensado para ser utilizado por los padres y los hijos. Los cuatro temas están enfocados a través de la historia de dos jóvenes, Alex y Zeta, sus padres, y el genio de la tecnología, Hedvig. Cada capítulo contiene actividades educativas, incluyendo ejercicios en línea, juegos de preguntas, reglas de oro y enlaces útiles.

Lea la historia en voz alta con sus hijos y juntos trabajen con las actividades propuestas. Al final de cada capítulo, usted puede utilizar las tarjetas de situación correspondientes para provocar una discusión con sus hijos con el propósito de aumentar aún más la comprensión del contenido.

Cuando sus hijos hayan trabajado exitosamente con todo el contenido del kit de herramientas, recompénselos con el establecimiento de un acuerdo sobre un conjunto de reglas de oro y haga que todos firmen el certificado familiar. Finalmente, los niños pueden decorar los cuadernillos con pegatinas de emoticonos.

Su feedback es valioso para nosotros. Por favor no dude en ponerse en contacto con su centro local Insafe (PROTEGELES) en relación a preguntas o comentarios. ¡Le deseamos a usted y a su familia la mejor diversión mientras doman Internet!

Le deseamos una segura navegación,

Firma: El equipo de PROTEGELES

protegeles.com

B. Orientación para padres y tutores

1. La prevención brinda seguridad

UN ORDENADOR EN EL HOGAR

Un ordenador en el hogar puede ser un excelente recurso educativo y recreativo para toda la familia. Colocar el ordenador en un lugar de uso común en la casa, como por ejemplo el salón, y establecer reglas específicas en relación a las condiciones y el tiempo a pasar frente a la pantalla, ayuda a los miembros jóvenes de la familia a mantenerse seguros.

Recuerde que sus hijos pueden acceder a **Internet** en los hogares de sus amigos, en cibercafés, etc. Es la razón por la que es importante que establezcan un código de conducta seguro y confiable que ellos puedan aplicar en cualquier momento, en cualquier lugar.

PROTEGIENDO SU ORDENADOR

Puede lograrse una buena protección mediante una comprensión básica de las amenazas potenciales y un conocimiento de remedios simples. Estos remedios incluyen herramientas tecnológicas útiles y también el sentido común de los usuarios. Como todas las cosas, el

sentido común se desarrolla con la edad y la práctica.

Las cosas que usted y sus hijos están más acostumbrados a hacer en su ordenador en el hogar tal como utilizar **tarjetas de memoria** o **CD-ROMs**, abrir documentos **adjuntos** y **descargar archivos**, pueden involucrar riesgos. Estos riesgos se refieren principalmente a **programas informáticos** maliciosos (**malware**), diseñados para dañar su ordenador, robar información personal, o presentarle publicidad no solicitada.

Se presentan a los niños distintos tipos de malware: **virus**, **gusanos**, **caballos de Troya**, y **spyware**, y se les enseña a reconocer los síntomas de un ordenador infectado. Aprenden cómo prevenir una infección al acceder a Internet mediante un ordenador protegido por programas antivirus y **antiespía** actualizados. También se les advierte sobre la necesidad de ser cuidadosos al abrir los documentos adjuntos de correos electrónicos provenientes de remitentes desconocidos, descargar programas de Internet y utilizar tarjetas USB o CD-ROMs.

LUCHA CONTRA EL SPAM

El 80% de los correos electrónicos que circulan por Internet son **spam** (correo electrónico no solicitado) que puede fácilmente afectar a sus hijos. Publicar inadvertidamente una **dirección de correo electrónico** en la **Web** al utilizar un **grupo de noticias**, un sitio de **conversaciones en la red (chat)**, un **foro público**, un sitio de **redes sociales** o un **formulario online** puede generar spam. Ciertos programas específicos pueden recolectar direcciones de correo electrónico de la Web, para crear listas de correo, que después son utilizadas para distribuir spam de forma masiva. ¡Las compañías involucradas en estas actividades están generalmente ubicadas en sitios donde no hay legislación para prevenir el correo electrónico no solicitado!

Los correos electrónicos de spam, frecuentemente están vinculados a pornografía, productos farmacéuticos, transacciones financieras sospechosas, etc. Además, el spam también puede ser fuente de programas maliciosos. En la mayoría de los casos, los correos electrónicos de spam son distribuidos con intenciones fraudulentas. Aquí abajo proponemos algunos consejos para ayudarle a proteger a su familia:

- Utilice "**filtros de spam**". Su proveedor de correo electrónico usualmente ofrece opciones antispam que usted puede activar en su programa de correo electrónico. Póngase en contacto con su proveedor de correo electrónico para obtener información detallada. Verifique regularmente su **carpeta de correo basura** o **spam** para comprobar si algunos correos electrónicos inocentes han terminado allí. La tecnología no es infalible.
- Enseñe a sus niños a no abrir correos electrónicos provenientes de personas desconocidas. El spam casi siempre contiene ofertas y documentos adjuntos tentadores. Muéstreles cómo bloquear al remitente de un correo electrónico o simplemente pídales eliminar los correos electrónicos sospechosos.

NAVEGANDO POR LA RED

Incluso los niños muy pequeños pueden obtener beneficios de navegar por Internet por diversión y para visitar **sitios Web** educativos. Sin embargo, Internet también ofrece todo tipo de contenidos que no son siempre apropiados para su edad.

Los motores de búsqueda son muy buenos para ubicar contenidos en Internet. Aún así, debido a que la búsqueda se basa en una serie de palabras clave, también hace muy fácil ubicar contenidos no deseados. Una palabra clave que suena muy inocente puede devolver un sitio Web no tan inocente que contiene la palabra clave en cuestión. Aquí abajo hay algunos consejos para ayudar a sus hijos a navegar por Internet con mayor seguridad:

- Cree una cuenta de usuario especial para su hijo/a utilizando un sistema operativo, por ejemplo Windows, Linux, Mac OS, en el cual pueda activar controles parentales.
- Examine las características de controles parentales en su navegador de Internet y motor de búsqueda. Asegúrese de conocer las opciones ofrecidas por los ajustes familiares de esas herramientas.
- Proponga motores de búsqueda amigables con los niños, para los usuarios jóvenes de Internet que se encuentran bajo su tutela. Un ejemplo es *http://buscadorinfantil.com*
- Guarde las direcciones de los sitios Web preferidas por sus hijos en sus carpetas de favoritos (una opción del navegador). De ese modo les permite utilizar sus ubicaciones favoritas de la red una y otra vez sin tener que pasar por un motor de búsqueda.

Además de activar las características adicionales de control parental en su navegador y motor de búsqueda, usted puede utilizar un **filtro** adicional, un programa orientado a la protección de los menores de contenidos inadecuados en la Web. Pida consejo a su vendedor local, o busque en Internet **software** de prueba. También su proveedor de Internet le puede ofrecer un servicio de filtrado de contenidos a través del servidor (Canguronet-Telefónica).

Recuerde que nada puede reemplazar la orientación de los padres y los tutores de los niños. Las herramientas técnicas no son infalibles y pueden crear a veces un sentimiento falso de seguridad a menos que sean usadas conjuntamente con su sentido común.

El software de filtrado puede resultar tan restrictivo que puede bloquear contenidos inocentes. Podría bloquear e impedir el acceso de los niños a información referente a la Segunda Guerra Mundial, por ejemplo, al investigar para un trabajo del colegio porque la búsqueda conduce a sitios Web que describen violencia. Además, cualquier filtro que puede ser activado, puede ser desactivado por jóvenes inteligentes que con frecuencia son expertos en cubrir su rastro. Usted sólo se enterará de que esto está ocurriendo si aprende cómo utilizar el ordenador y el software.

Visite el sitio Web de SIP-Bench (ver sección de enlaces útiles), un estudio respaldado por la Comisión Europea en el marco del cual 30 herramientas de control parental y anti-spam fueron evaluadas para medir su efectividad protegiendo a niños entre 6 y 16 años de edad contra contenidos dañinos en varias aplicaciones de Internet: **navegación**, correos electrónicos, **transferencia de archivos**, conversaciones y *mensajería instantánea*.

Además de evitar el **contenido dañino**, usted debería asegurarse de que sus hijos no crean todo lo que ven o leen en Internet. En el cuadernillo de diversión familiar sugerimos que siempre visiten al menos 3 sitios Web para comparar los contenidos al buscar información en la red. También se les aconseja que mencionen sistemáticamente la fuente de la información hallada siempre que la usen para una tarea escolar.

REGLAS DE ORO PARA LOS PADRES DE NIÑOS QUE NAVEGAN

- Asegúrese de que su ordenador esté protegido por un cortafuegos además de programas antivirus y antiespía. Mantenga actualizados estos últimos y preste atención a

cualquier alerta que generen. Verifique si su Proveedor de Servicios de Internet (PSI, o ISP en inglés) ofrece herramientas antivirus y antiespía que puedan serle de utilidad.

- Utilice un filtro de spam en su programa de correo electrónico y mantenga su dirección de correo electrónico tan privada como sea posible, no publicándola en la Web. Evite los correos electrónicos provenientes de remitentes desconocidos y explore los documentos adjuntos por virus antes de abrirlos.
- Maximice las características de control parental de su software: en su sistema operativo, navegador de Internet, motor de búsqueda y programa de correo electrónico. Cree cuentas de usuario separadas para sus hijos. Asegúrese de que los ajustes de privacidad estén en el nivel más alto (examine el menú "Opciones" en su navegador).
- Considere el uso de un programa de filtrado adicional.
- Póngase en contacto con un experto tan pronto como su ordenador comience a comportarse extrañamente pues puede estar infectado. Su PSI/ISP debería también poder brindar orientación para padres.
- Envíe un informe a su línea de denuncia de Internet http://www.protegeles.com si entra en contacto con contenido no deseado en la red.
- Siéntese cerca de sus hijos cuando pueda mientras ellos estén navegando. Es un modo excelente de estimular la discusión y aumentar la confianza. Confronten el desafío de aprender juntos.
- Recuerde, estas reglas de seguridad se aplican tanto a usted como a sus niños. Incítelos a informarle sobre cualquier cosa que ellos piensen que les perturba o les extraña.

ENLACES ÚTILES

Sus hijos pueden realizar un curso sobre seguridad informática:
http://exprimelared.com

Para disfrutar de una navegación segura, conocer es clave: conocer los riesgos, conocer cómo protegerse y conocer más. Puede hallar más detalles en el sitio Web:
http://www.enlaredprotegete.com

También PROTEGELES ha creado un espacio para adultos y educadores que incluye un foro sobre esta temática:
http://www.ciberfamilias.com

En caso de encontrar contenidos que usted considere que puedan ser ilegales al navegar por la red, puede enviar un informe al servicio español de línea de denuncia:
http://www.protegeles.com

SIP-Bench:
http://www.sip-bench.org

2. Comunicándose

LAS PIEZAS DEL ROMPECABEZAS

¿Recuerda cuán importante era para usted mantenerse en contacto con sus amigos cuando estaba creciendo? Internet ofrece montones de nuevos lugares para encontrar amigos y ofrece nuevos modos de expresión y socialización mediante correo electrónico, compartir archivos, los blogs, y las redes sociales (por ejemplo MySpace, Facebook, Hi5, Habbohotel, tuenti), etc. Los adolescentes hoy usan la tecnología para probar nuevas cosas y socializar en un espacio que sienten como privado y libre de la vigilancia de sus padres.

El capítulo de comunicación introduce a los padres y a los niños al concepto de **información personal**, **privacidad**, interacciones positivas en la red y el manejo de riesgos tales como el contacto con extraños. La privacidad en la red tiene un vínculo cercano con el concepto de **cuentas** y **perfiles**. Una cuenta es lo que hace posible acceder a un servicio online.

Sin estar conectados, un billete de autobús, una tarjeta de gimnasio o de socio, contienen información personal sobre usted. Las cuentas y servicios en la red son similares. No puede abrir ninguno de los dos a menos que brinde algo de información personal que se usa para crear su "perfil de usuario". Es importante considerar que usted puede elegir tanto el tipo de información que desea presentar sobre usted mismo, como con quién desea compartir esta información.

La protección de su privacidad consiste en administrar qué desea que las personas conozcan sobre usted mismo en lugar de mentir sobre quién es usted. Los jóvenes son entusiastas acerca de comunicarse con amigos en la red y crear su imagen virtual. Sin embargo, no siempre comprenden el impacto que puede tener sobre ellos cuando hacen pública su información privada.

CREANDO UN PERFIL

El primer paso en la protección de la información personal es la creación de un perfil más seguro al reflexionar cuidadosamente sobre la información que incluirá y los ajustes de privacidad a aplicar.

Cree varias cuentas de correo electrónico para diferentes contextos en la red. Por ejemplo, al utilizar servicios en la red como conversaciones, mensajería instantánea, blogging, etc., anime a sus niños a utilizar una dirección de correo electrónico y un **apodo (nickname)** neutral. De este modo su hijo/a no utiliza una dirección de correo electrónico que revela su nombre completo.

Siempre mantenga en secreto las **contraseñas** de las cuentas. Asegúrese de que sus niños comprendan que no deben compartir sus cuentas personales con amigos que pueden hacer un mal uso de su confianza. Por otra parte, puede que desee conocer las contraseñas de sus hijos para poder supervisar sus cuentas. Hable con ellos acerca de esto.

Recuerde personalizar los **ajustes de privacidad** de su perfil/cuenta seleccionando que sea privada y no pública. Esto le brinda la oportunidad de controlar para quién será visible y con quién puede interactuar. Un perfil privado significa que usted puede administrar su **lista de contactos**. Enseñe a sus niños a aceptar solamente contactos de personas que ya conocen en la vida real.

Si sus hijos utilizan salas de conversación (chat), verifique que:

- haya **moderadores** en vivo presentes. La ausencia de moderadores significa una conversación insegura.
- haya herramientas para ignorar o bloquear a los participantes indeseados.
- haya una función de ayuda y **reporte** en el sitio Web a la que puedan acceder en caso de tener problemas.
- las reglas del servicio estén presentadas clara y visiblemente.

IMÁGENES Y CÁMARAS WEB (WEBCAMS)

Los niños deben comprender que su fotografía es una parte integral de su privacidad y que las imágenes digitales son extremadamente poderosas. Son fácilmente circulables y **manipulables**, y son muy difíciles de borrar una vez que han sido enviadas a través de un ordenador o un teléfono móvil, ¡podrían quedar en la red para siempre! Las cámaras Web deberían usarse cuidadosamente y los niños no deberían utilizar cámaras Web sin supervisión. Las herramientas de conversación mediante **cámaras Web** y los **directorios** pueden suponer riesgos. Usted y sus hijos deberían compartir sus imágenes personales solamente con personas que conozcan y en las que confíen, y siempre obtenga permiso antes de publicar una fotografía de alguien. No permita que sus hijos usen un ordenador y cámara Web solos en su habitación.

CONTACTO CON EXTRAÑOS

La gente que conoce en la Internet no es siempre quien dice ser. Enseñe a sus hijos a salvaguardar su privacidad en la red de la misma forma a como lo harían fuera de Internet. Usted establece reglas sobre cómo se comportan con los extraños en el mundo real, así que ¿por qué no deberían seguir las mismas reglas en Internet?

Sus hijos pueden crear una fuerte relación con amigos en Internet y tienden a confiar fácilmente en gente que muestra interés y entendimiento en relación a ellos incluso si no los conocen realmente. Consecuentemente, pueden sentirse muy tentados de conocer a esos nuevos amigos personalmente sin informarle a usted. Los niños frecuentemente no son conscientes del peligro de esos encuentros y pueden considerarlos triviales. Esto los

convierte en víctimas fáciles de **seducción de menores** en que han conocido en Internet. Los estudios muestran que muchos niños acuden solos a encontrarse con "amigos" que han conocido en Internet sin informar siquiera de ello a sus padres. Hable con sus hijos sobre esto para asegurarse de que no les ocurra a ellos. La comunicación es clave.

ETIQUETA DE LA RED o NETIQUETA (NETIQUETTE)

Etiqueta de la red hace referencia a los buenos modales en Internet y a tratar a otras personas en la red como le gustaría que lo traten a usted. Los niños pueden no comprender que pueden ofender a alguien accidentalmente en Internet. Desafortunadamente, algunas personas usan Internet y/o los teléfonos móviles para molestar y acosar a otros. Esto se llama acoso en la red o ciberacoso y puede afectar hasta a uno de cada cuatro niños (consulte el capítulo relevante para obtener más información).

LENGUAJE EN CONVERSACIONES (CHAT)

Al conversar en Internet los jóvenes usan un lenguaje singular, ¡lleno de **emoticonos** y **acrónimos**! Observe las tablas abajo para familiarizarse. 😂

Lista indicativa de **acrónimos** de las conversaciones, para obtener más información consulte los enlaces útiles:

hla: Hola	KLS: Que lo sepas
hlgo: Hasta luego	LAP: Lo antes posible
NV: Nos vemos	ls: Los/ las
X fa: Por favor	nl: En el/en la
K tl?: ¿Qué tal?	mñn: mañana
xq: Porque	F2t : Free to talk/ Libre para hablar
xa: Para	Bss : Besos
kls: clase	ly4e : Te querré siempre (love you forever)

Usted puede crear emoticonos combinando signos de puntuación y letras, vea los ejemplos aquí abajo::

Una sonrisa (con o sin nariz)	**:)** or **: -)** dos puntos, (guión), paréntesis

Una cara triste (con o sin nariz)	**:(** or **:-(** dos puntos, (guión), paréntesis
Cara guiñando el ojo (con o sin nariz)	**;)** or **;-)** punto y coma, (guión), paréntesis
Cara de sorpresa (con o sin nariz)	**: o** or **:-o** dos puntos, (guión), o minúscula
Gran sonrisa (con o sin nariz)	**:-D** or **: D** dos puntos, (guión), D mayúscula
Mostrando la lengua (con o sin nariz)	**: p** or **:-p** dos puntos, (guión), p minúscula

REGLAS DE ORO

- Tómese el tiempo necesario para descubrir cómo pasan el tiempo sus niños en Internet y haga que les muestren cómo se comunican con sus amigos.

- Enséñeles a salvaguardar su privacidad en la red mediante:

  - La creación de perfiles seguros con ajustes de privacidad activados
  - La protección de sus contraseñas
  - Sólo contactando y respondiendo a personas que conocen en la vida real
  - Siempre pedir el permiso de sus padres antes de subir imágenes de sí mismos o de su familia, casa, escuela, etc.
  - Compartir únicamente información personal como su número de teléfono, dirección, escuela, equipo de deportes, etc., con gente que conocen bien en la vida real.

- Coloque el ordenador de la casa en una habitación familiar de modo que usted pueda supervisar sus actividades en la red.

- Juntos, asegúrense de saber:

  - Cómo rechazar contactos o bloquear personas de una lista de contactos.
  - Las funciones de seguridad y de reportes que están disponibles en los sitios Web que usan.

- ¡Fomente la confianza mútua transmitiéndo a sus niños que pueden hablarle sobre sus errores de modo que puedan buscar soluciones juntos! Los errores son parte del aprendizaje.

ENLACES ÚTILES

Una página creada por PROTEGELES especialmente concebida para padres y donde se ofrece la posibilidad de contactar y trasladar sus dudas:
http://www.ciberfamilias.com

También pueden los padres y educadores obtener información sobre un uso seguro de Internet en:
http://www.enlaredprotegete.com

Comprenda el código de las conversaciones en línea visitando wikiHow:
http://www.wikihow.com/Understand-Chat-Acronyms

Consulte el informe Eurobarómetro 2007 sobre una Internet más segura para los niños:
http://ec.europa.eu/information_society/activities/sip/eurobarometer

3. Acoso en la red

UN INCIDENTE DE CIBERACOSO

La comunicación mediante Internet y los teléfonos móviles tiene montones de increíbles ventajas. Lamentablemente, puede también no ser una experiencia tan increíble. Sus niños pueden recibir o enviar mensajes con contenido que hiera sus sentimientos o los sentimientos de otros. Es importante que enseñe a sus hijos conductas socialmente aceptables. Incluso nuestros propios hijos no son siempre ángeles ;-)

El **ciberacoso** (ciber-bullying) es el uso de nuevos dispositivos y servicios de comunicación e información para acosar, amedrentar o intimidar a un individuo o grupo. Puede usarse correo electrónico, conversaciones en la red, mensajería instantánea, teléfonos móviles u otras herramientas digitales. En los entornos de juegos virtuales, los acosadores pueden atacar el avatar de su hijo, por ejemplo disparándole, robándole posesiones virtuales o forzando al avatar a comportarse de un modo no deseado.

Comúnmente, los niños describen problemas vinculados a la revelación de información privada en espacios públicos, por ejemplo publicando una fotografía privada o información personal en un foro público o sitio Web. Como ocurre en el caso del **acoso** en la escuela o en el patio de recreo, tal conducta no es aceptable y los padres, los educadores y los niños deben estar alerta y listos para responder. A diferencia del acoso tradicional, el acoso en la red puede afectar al niño/a incluso cuando no está en presencia de los acosadores. Por ejemplo, los acosadores pueden enviar mensajes amenazantes, a cuentas de correo electrónico de uso en el hogar y teléfonos móviles, en cualquier momento del día o del la noche.

Los padres pueden ayudar a promover un ambiente en el que el acoso no sea tolerado. Enseñe a sus hijos que mantener el anonimato en la red no significa que puedan actuar irresponsablemente. Necesitan conocer sus propios derechos y responsabilidades, y cómo respetar los derechos de otras personas.

Mantenga siempre un diálogo abierto con sus niños, de modo que puedan hablar sobre cualquier situación preocupante. ¡Las nuevas tecnologías, como Internet y los teléfonos móviles, pueden brindar una excelente oportunidad para la discusión y ser motivo de reflexión!

REGLAS DE ORO

- Evite las experiencias negativas asegurándose de que sus hijos comprendan cómo proteger su propia privacidad y de que respeten la privacidad de otras personas.
- Enseñe a sus hijos a no responder a mensajes intimidantes.

- Ayude a sus hijos a comprender qué tipo de mensajes y conductas podrían hacer que otros se sintieran mal, y cómo evitarlo.
- Asegúrese de que sepan cómo bloquear a contactos de su lista de contactos.
- Mantenga un registro de mensajes ofensivos, puede necesitarlo como una prueba importante.
- Averigüe las estrategias anti-acoso de la escuela de sus hijos. Trabaje junto con otros padres y maestros para prevenir el acoso y el ciberacoso.
- Manténgase en contacto con el entorno de sus hijos; conozca a sus amigos, los padres de sus amigos, sus maestros y compañeros de clase.
- Anime a sus hijos a comentarle sobre cualquier experiencia inquietante en la red o fuera de Internet. ¡Asegúreles de que incluso si hacen algo por descuido, usted estará allí para apoyarles y que juntos hallarán soluciones!
- Asegúrese de que sus hijos comprendan que nunca tienen la culpa si alguien los acosa.

ENLACES ÚTILES

PROTEGELES ha creado una línea de ayuda contra el acoso escolar donde se puede obtener información específica para padres:

http://www.acosoescolar.info/padres/index.htm

Así como la posibilidad de contactar con nuestro equipo de profesionales, psicólogos y pedagógos, expertos en este tema y recibir atención personalizada:
http://www.acosoescolar.info

4. Entretenimiento y Descargas

NO ES ORO TODO LO QUE RELUCE EN INTERNET

Internet es un espacio virtual para montones de actividades, incluyendo algunas comerciales. Si usted no permite que sus niños tengan todo lo que ven publicitado en TV, o todo lo que les impresiona en un negocio, entonces también debería enseñarles a no querer o creer todo lo que se publicita en Internet, por ejemplo, música y juegos, **tonos de llamada**, otros accesorios y la compra de servicios en la red.

Pasar tiempo con sus niños en Internet le brinda la oportunidad de explicarles que los productos tales como tonos de llamada, **fondos**, **mp3s**, **avatares**, etc, raramente son gratuitos. Donde sea que encuentre estos anuncios, muéstreles la letra pequeña para demostrarles que no deberían aceptar todo lo que se encuentra en la red.

Para suscribirse a cualquier servicio (gratuito o no), deberá rellenar un **formulario en la red** con información personal relevante. Sólo complete estos formularios cuando esté seguro sobre cómo será usada su información personal, y desaconseje a sus hijos rellenar y enviar estos formularios a menos que los cumplimenten juntos.

Las ventanas emergentes se utilizan con frecuencia para vender cosas en Internet. No son siempre malas, depende de si provienen de un sitio Web de confianza o no. Generalmente, si usted confía en el sitio Web, puede confiar en la ventana emergente. Sin embargo, algunas **ventanas emergentes** se utilizan para comercializar productos que no son de fiar o que conducen a cuestionarios en a red que recogen información personal. Enseñe a sus niños a cerrar las ventanas emergentes que no sean de confianza haciendo clic en la cruz roja en la esquina superior derecha.

JUGANDO A JUEGOS ONLINE

Los juegos online difieren de los juegos digitales más viejos porque requieren una **conexión de red** activa. Los niños pueden jugar a juegos que se encuentran en un CD/DVD en **sitios Web**, en consolas videoconsolas de juegos, en teléfonos móviles o en otros dispositivos portátiles.

Los juegos online incluyen desde juegos simples y bien conocidos como Pacman y Tetris hasta juegos de realidad virtual en los que varios usuarios juegan juntos en la red, creando contenidos e historias. Muchos de estos **juegos para múltiples jugadores** mantienen comunidades virtuales de jugadores. Esto puede exponer a los niños a riesgos asociados con encontrarse con gente que no conocen en Internet (ver el capítulo sobre Comunicación).

Los juegos tienen un papel importante en el desarrollo de los niños pues las habilidades sociales y el pensamiento estratégico se desarrollan en un entorno delimitado por reglas de juego. Muchos juegos digitales son atractivos e interactivos y son usados con propósitos educativos.

Sin embargo, no todos los juegos digitales son de buena calidad. Usted debe decidir qué tipos de juegos son más adecuados para sus niños. Y, fijando reglas, usted puede asegurarse de que la cantidad de tiempo que sus niños pasan jugando en Internet no sea en detrimento de otras actividades.

Existe un sistema de clasificación paneuropeo según edades para los juegos interactivos, PEGI online, donde los juegos son clasificados de acuerdo a edad y contenido. Varios fabricantes, incluyendo PlayStation, Xbox y Nintendo, apoyan el sistema, así como también los editores y desarrolladores de juegos interactivos de toda Europa. Busque sus especificaciones en la parte trasera de la caja de cualquier juego que compre para un niño, pero recuerde, no todo niño de 12 años es igual.

REGLAS DE OROS

- Anime a sus hijos a utilizar sitios Web que ofrecen contenido legítimo y explíqueles que todo no es lo que parece ser en la red.
- Explique los riesgos de descargar material de la red sin precaución.
- Asegúrese de que su ordenador esté protegido y siempre utilice un antivirus actualizado.
- Lea siempre la declaración de privacidad y las condiciones de uso antes de instalar algo. Verifique (en Internet) si el software que quiere descargar es de confianza.
- Cierre las ventanas emergentes que no sean de su confianza haciendo clic en la cruz roja que se encuentra en la esquina superior derecha. Nunca haga clic dentro de ellas.

NIÑOS Y JUEGOS:

- Establezca reglas en relación a la cantidad de tiempo que sus niños pueden jugar.
- Permítales jugar en una habitación familiar donde pueda mantenerlos a la vista.
- Supervise los hábitos de juego de sus niños. Si los vigila en el patio o el parque, ¿por qué no hacer lo mismo cuando juegan en espacios virtuales?
- Discuta el contenido del juego, qué características son similares a la realidad y cuáles no, ¿qué les hace disfrutar?
- Antes de comprar un juego para su hijo, asegúrese de verificar que el contenido sea apropiado para su edad (sistema paneuropeo PEGI o cualquier otro sistema de clasificación nacional).

Cuando sus hijos juegan a juegos en Internet con múltiples usuarios:

- Escoja sitios con reglas estrictas y moderadores presentes.
- Adviértales el no dar detalles personales a otros jugadores.
- Adviértales sobre no encontrarse con otros jugadores en la vida real a menos que estén acompañados por usted.
- Anime a sus niños a que informen sobre abuso, amenazas o lenguaje inapropiado, la presentación de contenido desagradable, o invitaciones a encontrarse fuera del juego.
- Retire a su hijo del juego o cambie el identificador en Internet de su hijo si algo dentro del juego o del modo en el que se desarrolla le hace sentir incómodo.

ENLACES ÚTILES

Aprenda más sobre los juegos en línea y el sistema de clasificación por edad PEGI:
http://www.pegionline.eu

Existe la posibilidad de descargarse una guía sobre videojuegos con consejos para padres a la hora de participar en el proceso de compra de los mismos en:
http://www.guiavideojuegos.es

Comprenda la jerga de los archivos TXT en el sitio Web “transl8it”:
http://www.transl8it.com

Comprenda mejor la jerga de la red visitando:
http://www.netlingo.com

C. Soluciones propuestas a las actividades

1. La prevención brinda seguridad

ACTIVIDADES COMENTADAS

Combina la imagen con las palabras: torre de ordenador, alfombrilla del ratón, pantalla, altavoces, **cámara Web**, impresora, placa USB (o placa de memoria), ratón, CD-Rom.

Un ejercicio de precalentamiento para familiarizar a sus niños con las distintas partes de un ordenador y otro hardware relacionado. Puede desarrollar a partir de él tanto como usted considere apropiado.

Pide a tus padres que te envíen un correo electrónico con un documento **adjunto**, o envía tú mismo uno. Practica lo siguiente: haz clic con el botón derecho del ratón sobre el documento adjunto y guárdalo en el escritorio de tu ordenador. Ve al escritorio, haz clic con el botón derecho sobre el documento y haz clic en **escanear**. Cuando te asegures de que el documento es seguro, puedes abrirlo. Recuerda: clic con botón derecho y GUARDAR - ESCANEAR - ABRIR

Envíe un correo electrónico a la dirección de correo electrónico de su hijo o a su propia dirección y adjunte un archivo. Que su niño siga las instrucciones en el ejercicio para

guardar el documento haciendo clic con botón derecho sobre él sin abrirlo. Después de guardar el archivo en el Escritorio o en una carpeta del ordenador tal como Mis documentos, muéstrele al hijo cómo hacer clic con botón derecho una vez más en el documento para explorarlo por si tiene virus antes de abrirlo para fomentar hábitos seguros.

Sigue el consejo de Hedvig y aprende cómo describir tu dirección de correo electrónico cuando realmente necesites publicarla en la red. Esto es para evitar que tu correo electrónico sea registrado automáticamente y usado por quienes envían spam. Por ejemplo: cybercat.smith@mymail.com = cybercat punto smith arroba mymail punto com. Para practicar, describe las direcciones de correo electrónico que tienen en la familia: tu correo electrónico, el correo electrónico familiar, el correo electrónico de tu madre, el correo electrónico de tu padre.

Para evitar que su dirección de correo electrónico sea registrada automáticamente por software usado para distribuir spam, descríbala en lugar de escribirla tal como es. Que su hijo practique esta técnica tal como se sugiere arriba. Tenga en mente, sin embargo, que su hijo debería evitar de publicar su correo electrónico en Internet, y si lo hace, debería utilizar uno que no revele su nombre (ver capítulo de Comunicación).

Para ayudar a Zeta a comprender antes de que Hedvig avance más, mira las actividades en la caja y traza un círculo alrededor de aquellas cosas que sólo puedes hacer si estás conectado a Internet.

Sus hijos más pequeños pueden no comprender claramente qué actividades requieren una conexión de red y cuáles no. Escribir un texto no requiere de una PC conectado, pero conversar sí. Puede escuchar música en su PC usando un CD o un archivo de música almacenado en su ordenador, pero también puede directamente escuchar música en Internet. Sus hijos deben marcar sólo aquellas actividades para las cuales es esencial una conexión de red.

Junto con tus padres, escribe http://www.buscadorinfantil.com en tu navegador. Busca información sobre Tiranosaurio Rex, e intenta descubrir cuándo vivió este dinosaurio en la Tierra. También intenta hallar una buena imagen de un Tiranosaurio. No te olvides de verificar en tres sitios Web diferentes.

Guardar y organizar sitios interesantes en la carpeta de Favoritos (opción de la barra de herramientas del navegador) es una muy buena forma de reducir la necesidad de que sus niños pequeños busquen información en Internet.

¿LO HAS HECHO CORRECTAMENTE?

1: (protegido) 2: (virus), (desconocido), (descargando), (infectado), (placa de memoria), (desprotegido) 3: (extrañamente) 4: (saber), (adjuntos), (asuntos), (spam) 5: (único), (spam) 6: (primero), (tres), (comparar), (cualquiera), (publicar) 7: (antivirus), (anti-espía) 8: (hablar), (padres) 9: (decir)

SOLUCIONES SUGERIDAS A TARJETAS DE SITUACIÓN

SITUACIÓN 1. Nunca navegues por Internet si tu ordenador no está protegido por un software actualizado de antivirus y anti-espía. Es como tener una frontera sin guardias de frontera; tu ordenador podría quedar infectado por programas dañinos, tales como virus, caballos de Troya, gusanos o espía.

SITUACIÓN 2. Mantén los ojos abiertos frente a correos electrónicos que te llegan de personas que no conoces y que contienen documentos adjuntos o correos electrónicos que 'prometen todo', ¡muy probablemente sean spam! El spam puede infectar tu ordenador con programas dañinos, tales como virus, caballos de Troya, gusanos o spyware. No abras esos correos electrónicos. En cambio, bloquea al remitente haciendo clic con el botón derecho del ratón sobre el correo electrónico y seleccionando 'Bloquear remitente' o simplemente elimínalos.

SITUACIÓN 3. Cuando busques información en Internet, no confíes inmediatamente en la primera página que obtengas como resultado de la búsqueda. Verifica al menos en tres sitios diferentes y compara la información que halles en ellos. Recuerda: cualquiera con acceso a Internet puede crear y publicar información en la red. Cuando escribas un informe o una tarea, siempre debes mencionar la fuente de la información y las imágenes que has usado... eso es lo que un verdadero científico haría.

2. Comunicándose

ACTIVIDADES COMENTADAS

Califica cómo son de **privado** los siguientes datos para ti: tu número telefónico, tu color de pelo, tu nombre, el país en el que vives, la escuela a la vas, tu dirección, el nombre de tu mascota, las profesiones de tus padres, tu dirección de correo electrónico, tus fotografías, tu edad.

¿Tienen sus hijos la misma percepción de privacidad que usted? Los tres colores representan información muy privada (rojo), bastante privada (naranja) y no tan privada (verde).

Ayuda a Zeta a crear una contraseña realmente buena siguiendo los consejos de Hedvig.

Las buenas contraseñas deben contener un conjunto aleatorio de caracteres diferentes (números, letras y signos de puntuación) y siempre deben ser mantenidas en secreto.

Sigue el ejemplo de Zeta y crea un perfil seguro. Luego crea un ejemplo de uno inseguro.

Que sus hijos creen un perfil seguro y luego uno menos seguro que revele información privada. Recuerde a sus hijos que crear un perfil seguro no los protege si ellos no continúan protegiendo su privacidad al comunicarse en la red.

Mira esta imagen y escribe lo que puedes adivinar acerca de esta persona.

¿Qué información personal puede deducirse a partir de una imagen? Con frecuencia, los niños no tienen conciencia del poder de las imágenes.

Verifique que sus hijos han comprendido que ponerse en contacto con extraños en Internet puede involucrar riesgos.

¿Cómo te gustaría que la gente te trate en línea? (1.... 2.... 3....)

Asegúrese de que sus hijos comprenden que deben tratar a otros como ellos desearían que los tratasen a ellos.

DESCIFRA EL CÓDIGO: Descubre qué significan algunos de los acrónimos más populares usados en conversaciones en línea uniéndolos a sus significados.

Mejore su comprensión de los acrónimos consultando el capítulo Comunicándose / Etiqueta de la red, lenguaje en conversaciones.

Usa combinaciones del teclado para simbolizar estos emoticonos: Una cara sonriente - Una cara triste - Cara guiñando un ojo - Cara de sorpresa - Gran sonrisa - Mostrando la lengua.

Consulte el capítulo Comunicándose / Etiqueta de la red, lenguaje en conversaciones para obtener más información.

¿LO HAS HECHO CORRECTAMENTE?

1: (perfil) 2: (privacidad), (responsable) 3: (extraños), (decir) 4: (Etiqueta de la red), (tratado) 5: (emoticono) 6: (contraseña), (puntuación) 7: (secreto) 8: (negarse) 9: (saber)

SOLUCIONES SUGERIDAS A LAS TARJETAS DE SITUACIÓN

SITUACIÓN 4. Cuando uses Internet, tu perfil, o la información que das sobre ti, puede llegar a decenas, cientos, miles o incluso millones de personas. Es la razón por la que es importante escoger cuidadosamente la información que muestras sobre ti. Sólo da información personal a gente en la que confías y que conoces bien en la vida real.

SITUACIÓN 5. Mike probablemente compartió la contraseña de su correo electrónico con su amigo, quien luego decidió atacarlo enviando correos electrónicos desagradables en su nombre. ¡Siempre mantén en secreto las contraseñas a menos que no tengas problemas con que otras personas lean tus correos electrónicos o que se hagan pasar por ti y digan cosas que tú nunca dirías!

SITUACIÓN 6. Encontrarse en persona con un extraño no es una muy buena idea. Pero si realmente crees que puedes confiar en un amigo virtual que quiere conocerle, coméntaselo a tus padres y asegúrate de que uno de ellos te acompañe. Ningún amigo real con intenciones honestas tendría problemas con ello. Sólo es un problema para las personas que tienen algo que ocultar.

3. Acoso en la red

ACTIVIDADES COMENTADAS

Haz un dibujo de la invitación que Alex recibió de sus maestros. Muestra el logo y el eslogan anti-acoso que la escuela está usando para la semana anti-acoso.

Permita que sus hijos sean creativos y que dibujen en el cuadro vacío.

Sigue el ejemplo de Alex y da cinco razones que te harían sacarle una "tarjeta roja" a alguien.

Discuta con sus hijos qué tipo de conductas consideran inaceptables..

¿LO HAS HECHO CORRECTAMENTE?

1: (justo), (arruinar) 2: (hablando) 3: (bueno) 4: (acoso en Internet) 5: (bloquear) 6: (saber) 7: (responder)

SOLUCIONES SUGERIDAS A TARJETAS DE SITUACIÓN

SITUACIÓN 7. Este definitivamente no es un modo aceptable de utilizar tu teléfono móvil. No hagas circular mensajes, imágenes u otro material que pueda ser hiriente. Siempre trata a otros como te gustaría que te tratasen a ti. En una situación así, siempre habla con tus padres o con otro adulto en quien confíes.

SITUACIÓN 8. Alex debería decirle a su amigo que la mala conducta del acosador no es error suyo. No debería responder a los mensajes del acosador, pero debería guardarlos como prueba y mostrárselos a sus padres o maestros. Alex también debería hablar sobre esto con sus padres, quienes pueden apoyarlo al ayudar a su amigo.

SITUACIÓN 9. La etiqueta de la red se basa en tratar a otros en la Web como quisieras que te trataran a ti. Estamos seguros de que has aprendido lo suficiente ahora como para ayudar a Zeta en esta tarea.

4. Entretenimiento y Descargas

ACTIVIDADES COMENTADAS

Abre tu buscador favorito. Ingresa "tonos de llamada gratis" o "juegos gratis", y observa qué recibes. **Visita algunos sitios Web. ¿Puedes hallar alguna trampa?**

Practique haciendo una búsqueda con las palabras clave ofrecidas y verifique los sitios Web que encuentre, buscando trampas comerciales. Observe cómo se omite la información en las letras pequeñas en los eslóganes de publicidad.

¿Cuál es tu juego de ordenador favorito? Comprueba si tus padres lo conocen y pueden describirlo. Si no tienen ninguna pista, explícaselo primero y haz luego que escriban una breve descripción. ¿Lo comprendieron correctamente? ¿Cuántos puntos les darías de uno a diez? .../10. Los padres completan una síntesis del juego favorito del niño, el niño hace un dibujo del juego.

¿Sabe realmente a qué tipo de juegos juega su hijo en Internet? ¿Sabe cuál es su juego favorito? ¡Deje que pongan su entendimiento a prueba!

¿LO HAS HECHO CORRECTAMENTE?

1: (gratis) 2: (formularios) 3: (trampas) 4: (formularios en la red) (personales) 5: (cruz) 6: (ignorar) 7: (privacidad) 8: (compartir), (tú mismo) 9: (pregunta)

SOLUCIONES SUGERIDAS A LAS TARJETAS DE SITUACIÓN

SITUACIÓN 10. Los test en la red pueden ser una forma muy buena de recabar la opinión del usuario. Sin embargo, si se le pide al usuario que facilite información, debería quedar claramente definido el propósito de la encuesta. Aconseja a tus hijos no rellenar cuestionarios en Internet a menos que tengan claro el contexto en que se piden. Aún procediendo de esta manera, deberán tener mucho cuidado de no revelar datos personales (ver el capítulo de comunicación).

SITUACIÓN 11. Hay servicios gratuitos en Internet, pero los tonos de llamada, los fondos de pantalla, MP3s, avatares y semejantes es probable que no sean gratuitos. Si Alex mira mejor el sitio Web, probablemente descubrirá letras muy pequeñas, informándole sobre el costo real del servicio. Los tonos de llamada, los juegos de preguntas, otros juegos, etc., son todas excelentes formas de atraer engañosamente a las personas a suscribirse a servicios supuestamente 'gratuitos' que, en realidad, les costarán dinero.

SITUACIÓN 12. Alex debe recordar mantener privada su identidad cuando juega en línea con otras personas que no conoce de la vida real. No debe dar información sobre dónde vive, la escuela a la que concurre, su apellido, etc. También debería informar a sus padres sobre los juegos a los que está jugando y nunca debería descargar ningún juego de Internet sin preguntarles, pues esto podría dañar el ordenador del hogar.

D. Glosario

Acosar: acoso a través de daño, amenazas, comentarios sexuales, ataque físico y lenguaje peyorativo repetidos perpetrados por uno o más acosadores.

Acoso cibernético (Ciber-bullying): se refiere al acoso efectuado a través de medios electrónicos, usualmente mediante mensajería instantánea y correo electrónico. Puede involucrar ataques, amenazas, comentarios sexuales, y lenguaje peyorativo. Los acosadores en la red pueden publicar información de contacto personal de las víctimas e incluso hacerse pasar por ellas y publicar material en su nombre con el propósito de calumniar o ridiculizar.

Acrónimo: una abreviatura que consiste en las primeras letras de cada palabra de una frase o expresión. Frecuentemente se usan acrónimos en las conversaciones en línea para hacer más rápida la comunicación. Por ejemplo, K tl, mñn, xq (ver capítulo sobre comunicación).

Adjunto: un archivo de ordenador que se envía junto con un mensaje de correo electrónico. Los gusanos y los virus usualmente son distribuidos como ficheros adjuntos de correo electrónico. Los correos electrónicos de remitentes desconocidos con ficheros adjuntos deben ser considerados como sospechosos.

Ajustes de privacidad: conjunto de detalles de privacidad específicos de una cuenta que usted puede editar para mejorar la privacidad que le proteja contra la revelación de información personal, cookies, etc.

Ajustes de seguridad (de un perfil): un conjunto de opciones personalizables de seguridad, vinculadas a su perfil en línea (ver definición). Generalmente estas opciones se relacionan con la apertura de imágenes y archivos, la identificación de proveedores de información de confianza

y el nivel de permisos para acceder a contenido para adultos.

Ajustes familiares: también conocidos como controles parentales. Ajustes usados para personalizar un navegador u otra herramienta usada para la Web, diseñados para hacerla más amigable para los niños mediante el uso de características como filtrado de contenidos, limitación de tiempo, control de juegos, etc.

Alerta: una pequeña caja que aparece en la pantalla para darle información o para advertirle acerca de una operación potencialmente dañina, por ejemplo, nuevo correo electrónico o el estado de su protección antivirus.

Antivirus: un programa informático que intenta identificar, aislar, bloquear y eliminar virus informáticos y otro software malicioso. El antivirus inicialmente escanea los archivos para buscar virus conocidos y luego identifica conductas sospechosas de programas informáticos para indicar una infección.

Antiespía (Anti-spyware): un programa que combate los programas espía (spyware). El programa escanea toda la información entrante buscando programas espía y luego bloquea las amenazas que encuentra o suministra una lista a partir de la cual eliminar las entradas sospechosas.

Apodo (nickname): sinónimo de nombre de pantalla e identificador. Representa al usuario de un servicio en Internet y lo define el usuario mismo. Representa a los usuarios en listas de contacto, salones de conversación en la red, etc. Los apodos, si están bien escogidos, pueden proteger su anonimato en Internet.

Archivo de ordenador: un archivo o conjunto de información de información relacionada (documentos, programas, etc.) almacenado en un ordenador bajo su propio nombre de archivo. Los archivos de ordenador pueden considerarse como el equivalente en la actualidad a los documentos en papel que eran almacenados en archivos de oficina y de bibliotecas.

Ataque ("flaming"): una interacción hostil e insultante entre usuarios de Internet. Con frecuencia tiene lugar en foros de discusión, espacios de conversación en línea (Internet Relay Chat, o IRC) o incluso mediante correo electrónico.

Autor: el creador de una obra literaria o audiovisual, un software, etc. Los derechos de autor, el copyright, protege las creaciones de los autores contra la reproducción ilegal.

Avatar: el perfil de un usuario representado por un nombre de usuario más una imagen, icono, o un personaje en 3D en juegos informáticos en Internet y mundos virtuales.

Barra de herramientas: conjunto de íconos o botones que son parte de la interfaz de un programa informático. Las barras de herramientas sirven como una interfaz fácil de utilizar y que está siempre disponible para realizar funciones frecuentes.

Blog: abreviatura de weblog. Un sitio Web en el cual un individuo o un grupo generan contenido, usualmente con frecuencia diaria, consistente en textos, imágenes, archivos audiovisuales y enlaces.

Bloguear: el acto de escribir o actualizar tu blog.

Caballo de Troya: código malicioso, malware, que puede introducirse en su ordenador oculto detrás de operaciones que aparentemente son inofensivas tal como juegos o incluso programas de rastreo de virus. Los troyanos no se replican a sí mismos pero típicamente han sido diseñados para obtener acceso

a datos delicados o destruir datos, y pueden borrar un disco duro o robar información confidencial.

Cámara Web (o Webcam): una cámara que puede transmitir video a través de la Web, en mensajería instantánea, aplicaciones de videoconferencia informática, plataformas de conversación en Internet, etc. Las cámaras accesibles mediante la Web incluyen a las cámaras digitales que suben imágenes a un servidor Web, ya sea contínuamente o a intervalos regulares.

Carpeta: una entidad en un sistema de archivos que contiene un grupo de archivos y/o otros directorios. Las carpetas pueden contener múltiples documentos y se usan para organizar información.

Carpeta de correo basura o spam: en una casilla de correo electrónico, el sitio donde se almacenan los correos electrónicos considerados como spam o correo basura.

CD-Rom: acrónimo del inglés para "memoria de sólo lectura en disco compacto". Es un Disco Compacto no grabable que contiene datos que pueden ser leídos por un ordenador. Los CD-ROM son usados para distribuir software informático.

Compartir archivos: intercambio de archivos en la red entre usuarios de ordenadores. El término incluye el ofrecimiento de archivos a otros usuarios (subir) y copiar archivos que se encuentran disponibles en Internet a un ordenador (descarga). Típicamente, los archivos se comparten mediante redes P2P ("peer-to-peer").

Conexión a Internet: se refiere a los medios a través de los cuales los usuarios se conectan a Internet. Algunos métodos comunes de acceso a Internet incluyen la conexión telefónica, líneas T, Wi-Fi, satélite y mediante teléfonos móviles.

Contenido dañino: imágenes, textos, documentos, etc. cuyo contenido puede causar daño. Por ejemplo, las imágenes que muestran violencia son inadecuadas y dañinas para los niños y los menores.

Contenido ilegal: contenido en línea que es ilegal según la legislación nacional. Los tipos más comunes de este tipo de contenido son imágenes de abuso sexual de niños, actividad ilegal en los salones de conversación en línea (por ejemplo, seducción de menores), y sitios Web con contenidos de odio y xenofobia y apología del terrorismo.

Contraseña: una serie secreta de caracteres que permite a su propietario acceder a un archivo, ordenador, cuenta o programa, como medida de seguridad contra usuarios no autorizados (ver capítulo Comunicándose).

Control parental: ver definición de "ajustes familiares".

Conversación en Internet ("chat" en inglés): comunicación sincrónica a través de Internet mediante mensajes escritos, utilizando aplicaciones de conversación y de mensajería instantánea (por ejemplo, MSN).

Cookies: un archivo que un sitio Web coloca en su navegador de Internet. Cada vez que usted accede al sitio Web nuevamente, el cookie se envía de nuevo al servidor en el cual está almacenado el sitio Web. Los cookies informan sobre sus preferencias de sitios Web y se usan en sistemas de compras en línea. Rechazar los cookies puede impedir el acceso a ciertos sitios Web.

Copyright: un conjunto de derechos exclusivos que regula el uso de una idea, obra o información. El copyright se representa con el símbolo "©".

Correo basura: mensajes de correo electrónico no deseados y casi idénticos que son enviados a las personas mediante su dirección de correo electrónico. Como Internet es pública, en realidad hay poco que puede hacerse para prevenir el correo basura, así como es imposible prevenir el spam.

Correo electrónico: un medio de comunicación electrónica escrita que le permite enviar mensajes con cualquier tipo de archivo de ordenador adjunto: texto, imágenes, audio y otros.

Cortafuegos ("firewall"): un dispositivo de hardware (integrado en su enrutador ("router") o software (instalado en su ordenador) configurado para prevenir que usuarios no autorizados accedan a un ordenador o a una red de ordenadores conectados a Internet.

Cracker: una persona que ingresa a la fuerza e ilegalmente en sistemas informáticos.

Crackear: copiar ilegalmente software comercial forzando la función de protección de copyright.

Cuenta: una cuenta le permite autenticarse y autorizarse para utilizar servicios en la red mediante un nombre de usuario y una contraseña. Puede utilizar su sistema operativo para crear cuentas de usuario diferentes para cada miembro de la familia.

Descargar: se refiere al proceso de copiar un archivo desde un servicio en Internet a un ordenador.

Dirección de correo electrónico: una ubicación virtual en la que pueden entregarse mensajes de correo electrónico. Las direcciones de correo electrónico consisten en dos partes, separadas por el símbolo @.

Directorio: una unidad organizacional que su ordenador utiliza para organizar las carpetas y los archivos dentro de una estructura jerárquica. Por ejemplo, Mis documentos, Mis imágenes, etc.

Emoticono: una imagen o icono usado para transmitir sentimientos y emociones, por ejemplo, una cara sonriente. Puede simbolizarse usando caracteres de teclado y signos de puntuación estándar o mediante caracteres prediseñados incluidos en salones de conversación en Internet, sistemas de mensajería instantánea, teléfonos móviles, etc.

Enlace: una referencia a un documento que se encuentra disponible en Internet (página Web, documento de texto, imagen, etc.). Cuando usted hace clic en el enlace, obtiene una nueva página o un sitio Web totalmente diferente. Los enlaces de texto aparecen típicamente en azul y subrayados, pero también pueden aparecer en cualquier otro color y no estar subrayados. Las imágenes también pueden hacer de enlaces a otras páginas Web.

Etiqueta de la red o Netiqueta ("netiquette"): etiqueta utilizada en Internet que determina las reglas cívicas para las comunicaciones en la red.

Escanear: la acción o proceso de convertir material impreso en archivos digitales mediante el uso de un escáner. Esta conversión le permite visualizar el material como un archivo electrónico en su ordenador y distribuirlo en la red.

Favoritos: una carpeta personalizable del navegador, donde usted puede guardar enlaces o marcadores interesantes. Los marcadores pueden organizarse en subcarpetas y/o marcarse con palabras clave para simplificar su búsqueda.

Filtro: una aplicación que regula el acceso a la información o a servicios específicos de Internet, ad-

vierte acerca de sitios Web problemáticos, hace un seguimiento de la navegación del usuario, bloquea sitios que implican riesgo e incluso desconecta un ordenador totalmente. Los sistemas de filtro pueden instalarse en ordenadores independientes, servidores, teléfonos con acceso a Internet, etc.

Filtro de spam: una aplicación que evita que los mensajes de spam se almacenen en su bandeja de entrada de correo electrónico.

Fondo de pantalla (o de escritorio): un patrón o imagen u otra representación gráfica que forma el fondo de la pantalla de su ordenador.

Formulario (formulario en la red): un documento con formato que contiene campos en blanco que usted puede llenar con información. El formulario electrónico puede llenarse con texto libre o seleccionando alternativas de listas preestablecidas (desplegables). Después de enviarse, los datos son entregados directamente a una aplicación de procesamiento que los incorpora a una base de datos.

Foro: un grupo de discusión en línea en el que participantes con intereses comunes pueden intercambiar mensajes abiertamente acerca de diversos temas.

Freeware y shareware: en general, el software está protegido por copyright y por lo tanto no puede ser descargado. Freeware significa que el poseedor del copyright del software da su consentimiento para que el software sea usado por cualquiera sin cargo. Shareware significa que el poseedor del copyright da su consentimiento para que el software sea usado por cualquiera durante un período de prueba. Luego de ese período, el usuario debe pagar un valor para seguir utilizando el servicio.

Grupo de noticias ("newsgroup"): ver definición de foro.

Gusano: un tipo especial de virus que se replica a sí mismo, que puede distribuirse sin intervención del usuario a través de muchos ordenadores y puede dañar una red, consumir un tremendo ancho de banda, apagar un ordenador, etc.

Hacker: término usado popularmente para referirse a una persona que se involucra en crackear (ver 'cracker'). También puede usarse en los círculos informáticos para describir a una persona que es un entusiasta de la informática.

Hardware: la parte física de un ordenador, a diferencia del software informático que se ejecuta en el hardware. Puede ser interno: placas madre, discos rígidos y RAM (frecuentemente referidos como componentes), o externo: monitores, teclados, impresoras, etc. (también llamados periféricos).

Información personal: cualquier información que puede ser vinculada a una persona. Si debe obtenerse, procesarse y almacenarse información personal en la red, los propósitos deben ser declarados explícitamente.

Informar (o Reportar): una función que permite a los usuarios de espacios virtuales públicos reportar un problema (técnico, conducta inaceptable de un usuario, contenido ilegal, etc.) al moderador o al administrador de un sitio Web (llamado "webmaster").

Internet: es una red mundial, públicamente accesible, de redes de ordenadores interconectadas, mediante la cual tiene lugar la transmisión y el intercambio de datos. Involucra redes nacionales, académicas, de negocios y gubernamentales más pequeñas que pueden ofrecer varios servicios tales como información, correo electrónico, conversación en la red, transferencia de archivos, etc.

Juego de ordenador: un juego creado por desarrolladores de juegos y que se juega en un ordenador. Un juego online se define como un juego de ordenador que requiere de una conexión de red activa para poder jugarse. Los juegos online pueden aceptar interacción entre múltiples jugadores.

Juegos masivamente multi-jugador (Massively Multiplayer Games o MMG): juegos que ofrecen un mundo rico en tres dimensiones poblado de miles de jugadores que asumen los roles de personajes ficticios y que compiten entre sí. Los juegos de rol son los predominantes en esta categoría, en los que los participantes crean o siguen historias colaborando entre ellos.

Línea de ayuda: un servicio de correo electrónico y a veces de ayuda ofrecido en varios países por organizaciones de protección de la infancia y por los miembros de la red Insafe. Los niños pueden informar de preocupaciones acerca de contenido ilegal y dañino y de experiencias incómodas o atemorizantes en relación a su uso de las tecnologías en Internet.

Línea de denuncias anónimas (hotline): línea de apoyo telefónico o servicio basado en la Web en el que las personas pueden presentar denuncias sobre contenidos y/o usos de Internet catalogados como ilegales. Las líneas directas deben tener procedimientos efectivos y transparentes para procesar denuncias y tener el apoyo del gobierno, la industria, fuerzas de orden público y los usuarios de Internet en los países donde operan.

Lista de contactos: un conjunto de contactos en programas de mensajería instantánea y correo electrónico, juegos online, teléfono móvil, etc. Los contactos pueden agregarse, rechazarse y eliminarse.

Malware: abreviatura de software malicioso en inglés, hace referencia al software diseñado para infiltrar o dañar un sistema de ordenador sin el consentimiento informado del propietario. Incluye virus informáticos, gusanos, caballos de Troya, programas espía, adware deshonesto y otros tipos de software maliciosos y no deseados.

Manipulación: proceso de alteración de una imagen, archivo, fotografía o ilustración de modo aparente o no aparente. Hoy en día, existen muchas herramientas que pueden ser usadas para actuar sobre el contenido o forma de los datos, lo cual produce un resultado que difiere de la realidad.

Mensajería instantánea (MI o IM): una forma de comunicación electrónica instantánea y simultánea entre dos o más usuarios. La MI le permite comunicarse con una lista seleccionada de contactos. Cuando las personas en su lista de contactos se conectan, usted recibe un informe inmediato.

Motor de búsqueda: O buscador, es una herramienta utilizada para buscar información contenida en sitios Web. Los más conocidos son Google y MSN Search. Los motores de búsqueda han desarrollado preferencias específicas para cada usuario que pueden incluir ajustes de seguridad interesantes.

Móvil: un dispositivo electrónico de telecomunicaciones, también conocido como teléfono móvil, teléfono celular, GSM, teléfono inteligente (smartphone), teléfono portátil. Tiene la misma capacidad básica de un teléfono convencional fijo de línea. Hoy en día la mayoría de los móviles integran una cámara y muchos ofrecen acceso a Internet (mediante un servicio de pago).

MP3: es un formato de codificación específico para audio. Un archivo MP3 tiene aproximadamente una décima parte del tamaño del archivo de audio original, pero el sonido tiene casi la calidad de un CD. Debido a su tamaño pequeño y a su buena fidelidad, los archivos MP3 se han transformado en un medio popular de almacenar música tanto en ordenadores como en dispositivos portátiles.

Navegador: un programa usado para visualizar sitios Web. Internet Explorer, Netscape Navigator y Firefox son algunos de los navegadores más comunes para Windows, mientras que Safari es común en un entorno Mac. Las versiones más recientes de estos navegadores contienen características de control parental innovadoras.

Navegar: el acto de utilizar un navegador para ver sitios Web, o simplemente navegar por la red.

Nombre de pantalla: ver definición de Apodo.

Página de inicio: es la página Web que se carga automáticamente cuando se inicia un navegador Web. El término también se utiliza para referirse a la página inicial o principal de un sitio Web (ver definición).

Papelera de reciclaje: un directorio en un ordenador donde se almacenan temporalmente los archivos eliminados antes de que los usuarios los eliminen permanentemente. Usted debe eliminar regularmente los datos viejos y no deseados de la papelera de reciclaje para liberar espacio en el disco rígido, el almacenamiento interno de su ordenador.

Perfil: información personal acerca de un usuario en espacios de redes sociales, sistemas de mensajería instantánea, aplicaciones de conversación en la red, juegos online, etc. Los perfiles pueden ser públicos o privados y son personalizados por los usuarios para que los representen en espacios públicos.

Perfil de usuario: conjunto de información que describe a un usuario específico de un software, sitio Web u otra herramienta técnica. Generalmente incluye información tal como un nombre de usuario, una contraseña y otros detalles (por ejemplo, fecha de nacimiento, intereses).

Placa de memoria o USB: un dispositivo de almacenamiento de datos integrado con un conector USB (bus serie universal). Una placa de memoria generalmente es pequeña, ligera, movible y regrabable.

Pornografía infantil: la pornografía infantil, en España constituye un delito y se puede denunciar en la línea de denuncia española www.protegeles.com . Se pueden dar muchas acepciones de pornografía infantil, una de ellas sería una imagen que muestra a una persona que es un niño y que está involucrado o mostrado como estando involucrado en actividad sexual explícita.

Posesión virtual: un conjunto de objetos que se asigna a cada jugador de un juego. Cada jugador tiene posesión virtual de sus objetos mediante una terminal de ordenador que muestra el conjunto de objetos.

Privacidad: la capacidad de un individuo o grupo de controlar el flujo de información referido a sí mismo y por lo tanto de darse a conocer selectivamente. La privacidad a veces se relaciona con el anonimato, el deseo de permanecer sin ser conocido en el mundo público.

Privado: algo referente a un individuo o grupo que no debe ser revelado al público. Cuando algo es privado para una persona, usualmente involucra algo considerado inherentemente especial o personalmente delicado.

Procesador: o Unidad Central de Procesamiento (UCP, o CPU en inglés), es la parte de un ordenador que procesa datos, genera señales de control y almacena resultados. Junto con la memoria del ordenador, constituye la parte central de un ordenador.

Programa de ordenador: usualmente referido como software. El software consiste en una secuencia estructurada de instrucciones escritas por programadores de ordenadores, que permite a los ordenadores realizar tareas. Cuando usted compra un programa de ordenador, usualmente viene grabado en un CD-Rom (ver definición), un medio físico de almacenamiento de programas.

Protocolo de voz a través de Internet (VoIP: Voice over Internet Protocol): una tecnología que permite a los usuarios hablar a través de Internet, luego de descargar un software cliente. Las llamadas pueden ser sin cargo para los usuarios que se llaman entre sí usando el mismo cliente VoIP (por ejemplo Skype, Voicebuster). Estos programas usualmente ofrecen también funciones de conversación mediante texto y de compartición de archivos).

Puerto: es una interfaz en un ordenador usada para conectar con otro dispositivo. Los puertos pueden ser internos o externos. Los puertos internos conectan con un disco rígido o una red, mientras que los externos conectan con un dispositivo periférico tal como una impresora o un teclado.

Red: abreviatura de Internet.

Red P2P: una red P2P (o "peer-to-peer", en inglés) permite a aquellos que se conectan a ella a intercambiar archivos subiéndolos o descargándolos (ver definición). Es sólo uno de muchos medios a través de los cuales se intercambian archivos en Internet. Algunos servicios de intercambio de archivos son ilegales.

Redes sociales: plataformas virtuales que albergan comunidades de miembros que comparten intereses y actividades. Los miembros deben crear perfiles de usuario y pueden compartir herramientas para subir textos, imágenes u otros archivos, insertar mensajes en paneles de mensajes y participar en foros. Muchos sitios de red social están prohibidos para niños menores de 13 años de edad y ofrecen ajustes de seguridad para el perfil. Una red segura para menores es http://www.micueva.es

Registrarse: suscribirse a un servicio en línea: boletín de noticias, foro de discusión, correo electrónico, plataforma de conversación en línea, etc. Normalmente los usuarios deberían tener la opción de desconectarse cuando lo deseen.

Robo de identidad: robo de detalles personales (por ejemplo, nombre, fecha de nacimiento, número de tarjeta de crédito) y su uso ilegalmente.

Sala de conversación ("chat room"): espacio público virtual para comunicación en tiempo real. Gente de todo el mundo puede encontrarse en las salas de conversación y discutir mediante mensajes que escriben utilizando el teclado. Si sus hijos usan salas de conversación, asegúrese de que estén pensadas especialmente para su edad con supervisores y moderadores.

Second Life: una comunidad Web en 3D muy conocida, ofrecida por una compañía con base en los Estados Unidos de América, Linden Labs. Los usuarios pueden interactuar en línea mediante un avatar (ver definición), crear hogares, varios entornos, comerciar y ganar dinero virtual, etc. Ver www.secondlife.com.

Seducción de menores (en línea) o "grooming": el uso de las salas de conversación en línea (chat) para seducir a menores pretendiendo ser sus iguales. Los pedófilos inician conversaciones con víctimas potenciales para obtener información sobre su ubicación, intereses, pasatiempos y experiencias sexuales. Los depredadores usan varios medios para atraer a los niños a mantener conversaciones de naturaleza sexual.

SIP-Bench: un estudio apoyado por la Comisión Europea que probó 30 herramientas de control y anti-spam para medir su efectividad para proteger a los niños contra contenidos dañinos en Internet.

Sistema operativo: un programa que ejecuta las funciones básicas de un ordenador, haciendo posible que se ejecuten otros programas. Algunos ejemplos conocidos son Windows, Linux y Mac OS.

Sitio Web: una ubicación en la Web. Cada sitio Web contiene una página de inicio, que es el primer documento que usted ve al entrar al sitio. Los sitios usualmente contienen enlaces a archivos y sitios adicionales. Los sitios Web son propiedad de y gestionados por individuos, compañías u organizaciones.

Software: ver definición de programa de ordenador.

Software de prueba: software que usted puede probar antes de comprar. Las versiones de prueba del software usualmente ofrecen toda la funcionalidad de la versión regular, pero sólo pueden ser usadas por un tiempo limitado.

Spam: correo electrónico no deseado, usualmente de carácter comercial, enviado en grandes cantidades. El envío de spam a otras personas es claramente una de las violaciones más notables de Internet.

Spyware: malware adjuntado secretamente a archivos que se descargan de Internet, que se instala en el ordenador y controla su actividad. Envía la información a una tercera parte, que usualmente se trata de compañías interesadas en definir perfiles personales para enviar publicidad u otra información, o a crackers que quieren obtener acceso a información privada.

Suscribirse: registrarse voluntariamente en un servicio o actualización de noticias mediante el cual se enviará información directamente a su bandeja de entrada personal de correo electrónico.

Tono de llamada (o Timbre): un sonido utilizado por un teléfono móvil para anunciar llamadas entrantes. Existe una gran variedad de tonos y música personalizable disponible para que los propietarios de teléfonos móviles los descarguen, frecuentemente bajo pago de un precio, y los usen.

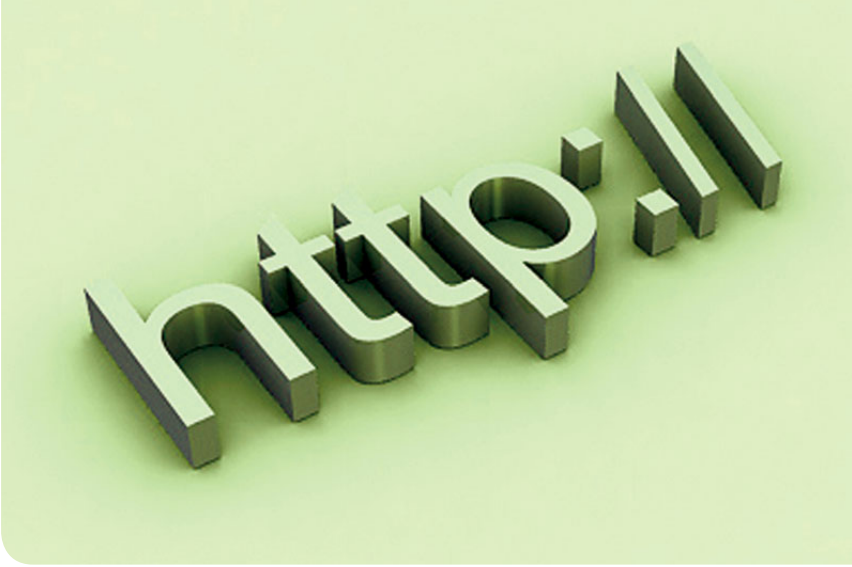
Transferencia de archivos: el acto de transmitir archivos a través de una red informática. Desde la perspectiva del usuario, la transferencia de archivos es referida frecuentemente como “subida” (uploading) o “descarga” (downloading).

URL (Uniform Resource Locator, o Localizador Uniforme de Recursos): la dirección de un sitio Web o archivo específico en Internet. No contiene caracteres especiales o espacios y utiliza barras tradicionales para indicar diferentes directorios. La primera parte de la dirección indica qué protocolo debe usarse, y la segunda parte especifica la dirección IP o el nombre de dominio donde se ubica el recurso.

Ventana emergente: una ventana que aparece repentinamente al visitar un sitio Web o presionar una tecla de función especial. Usualmente, las ventanas emergentes contienen un menú de comandos y permanecen en la pantalla hasta que usted selecciona uno de los comandos o la cierra haciendo clic en la cruz ubicada en su extremo superior derecho.

Virus: un tipo de código malicioso, malware, diseñado para propagarse con la intervención del usuario. Usualmente se distribuye mediante ficheros adjuntos de correos electrónicos pero también mediante herramientas de almacenamiento externo infectadas (placa USB, CD-Rom).

Web: abreviatura de World Wide Web (o “telaraña mundial”). Un conjunto de documentos en línea creados en HTML (Lenguaje de Marcado de Hipertexto, o Hypertext Markup Language en inglés) que contienen enlaces a otros documentos así como gráficos y archivos de audio y video. La Web es una parte de Internet.



E. Direcciones útiles

PROTEGELES

Sitio de la asociación PROTEGELES desde donde se pueden realizar denuncias sobre contenidos ilegales en Internet así como descargar estudios realizados sobre hábitos de consumo de los menores españoles en el uso de Internet y resto de tecnologías, y acceder a otras páginas creadas específicamente para menores en unos casos, o padres y educadores en otros
www.protegeles.com
www.exprimelared.com
www.enlaredprotegete.com

Líneas de ayuda contra la anorexia y bulimia promovidas en Internet y el acoso escolar
www.masqueunaimagen.com
www.acosoescolar.info

SITIOS SEGUROS PARA MENORES

Portal del Menor creado por PROTEGELES junto con el Defensor del Menor
www.portaldelmenor.es
Red social para menores creada por PROTEGELES donde los menores pueden crear sus espacios y contenidos
www.micueva.es

INSAFE

La red europea, de toma de conciencia vinculada a la seguridad informática, está orientada a capacitar a los usuarios para que puedan beneficiarse de los aspectos positivos de Internet evitando los riesgos potenciales:
http://www.saferinternet.org

protegeles.com ins@fe Apoyado por: chellomulticanal a Chellomedia company

Título: Kit e-seguro familiart • Creado por Insafe y apoyado por Liberty Global/UPC en 2008
Prefijo: 9789078209 • Id 51950 • ISBN-NÚMERO: 9789078209614 • EAN: 9789078209614