Navegación segura y uso responsable de Internet

SEGURIDAD EN LA NIÑEZ
Y ADOLESCENCIA

Navegación segura y uso responsable de Internet

Este documento tiene por objetivo acercar a padres, educadores y adultos a cargo de niños, niñas y adolescentes, información que ayude a conocer, detectar y prevenir conductas de riesgo para los menores en el uso de Internet y las nuevas tecnologías.

Av. Roque Sáenz Peña 511
C1035AAA
Ciudad Autónoma de Buenos Aires
Teléfono: (54-11) 4343-9001
www.sgp.gob.ar
info@sgp.gob.ar

Proyecto de Modernización del Estado
JEFATURA DE GABINETE DE MINISTROS

SGP Secretaría de la Gestión Pública
JEFATURA DE GABINETE DE MINISTROS

Jefatura de Gabinete de Ministros
Presidencia de la Nación

Navegación segura y uso responsable de Internet

SEGURIDAD EN LA NIÑEZ
Y ADOLESCENCIA

SGP Secretaría de la Gestión Pública
JEFATURA DE GABINETE DE MINISTROS

Jefatura de Gabinete de Ministros
Presidencia de la Nación

Autoridades

Presidenta de la Nación
Dra. Cristina Fernández

Jefe de Gabinete de Ministros
Dr. Aníbal Domingo Fernández

Secretario de la Gestión Pública
Dr. Juan Manuel Abal Medina

Subsecretario de Tecnologías de Gestión
Sr. Eduardo Thill

Índice

Introducción

El uso de Internet favorece la comunicación, la diversidad cultural y el abordaje a un nuevo universo de conocimiento.

El acceso a este nuevo escenario es una experiencia distinta y requiere que la familia, la escuela y el Estado estén preparados para guiar a las generaciones más jóvenes hacia un uso responsable, respetuoso y ético de Internet y las nuevas tecnologías en general.

La familia, los educadores y los adultos en su conjunto son los responsables de acordar con los niños, niñas y adolescentes los términos de su uso. Los especialistas aconsejan realizar un acuerdo o "contrato" sobre cuestiones básicas como tiempos, contenidos a los que se permite acceder y condiciones para la comunicación con nuevos usuarios con los que se contactan.

Este documento tiene por objetivo acercar información a padres, educadores y adultos a cargo de niños, niñas y adolescentes para ayudar a conocer, detectar y prevenir conductas de riesgo para los menores en el uso de Internet y las nuevas tecnologías.

Las recomendaciones para los adultos son válidas también para niños, niñas y adolescentes, ya que muchas conductas que vienen desde hace siglos, como el engaño y el robo de identidad, se repiten en Internet con idénticos objetivos. Sin embargo, el riesgo para los menores es mayor porque carecen de experiencia para enfrentar esas situaciones, con independencia de la forma en que se presenten.

Informar sobre los peligros potenciales de ninguna manera debe interpretarse como un desaliento para su uso, sino todo lo contrario. Internet es una herramienta maravillosa desarrollada por el hombre, relativamente nueva y de la cual todos aprendemos continuamente.

En este sentido, todos los actores que aportan contenido a la web, incluyendo a quienes cumplen un rol de intermediarios en la cadena de Internet (proveedores de servicios: hosting, conexión a Internet) tienen el compromiso moral de actuar sin olvidar que los niños, niñas y adolescentes también son sus usuarios.

En este documento hemos evitado incluir términos técnicos con el fin de facilitar su lectura, excepto cuando el uso de ellos resulta absolutamente imprescindible. En esos casos, el lector deberá remitirse a la sección Glosario, consignada al final del texto.

El material que se presenta a continuación ha sido elaborado por el equipo técnico de la Coordinación de Emergencias en redes Teleinformáticas (ArCERT) de la Oficina Nacional de Tecnologías de la Información (ONTI), perteneciente a la Subsecretaría de Tecnologías de Gestión.

Internet y nuevas tecnologías

El uso de Internet y las nuevas tecnologías nos brinda múltiples beneficios pero también nos expone a un conjunto de riesgos. Existen personas que, con el objeto de causar daño, aprovecharse de otros u obtener algún rédito, utilizan dichas tecnologías de forma maliciosa. Muchas de las amenazas por el uso de estas nuevas herramientas ya existían anteriormente y sólo fueron adaptadas a este nuevo entorno.

Resulta vital, entonces, conocer los riesgos a los cuales se exponen los niños, niñas y adolescentes con el objeto de tomar conciencia, estar prevenidos, protegerlos de cualquier posible daño y enseñarles el "buen uso" de las tecnologías.

Riesgos a los que se exponen niños, niñas y adolescentes

A continuación se enuncian los principales riesgos presentes en la actualidad:

- Violación a la intimidad

Las facilidades de acceso a la tecnología y el uso social por parte de los niños, niñas y adolescentes incentiva la exposición de mucha información personal sin restricciones y representa un riesgo si esos datos son utilizados con fines maliciosos. Una búsqueda de datos específicos podría llevar a encontrar información sensible de un niño, niña o adolescente (por ejemplo: domicilio, nombre de la escuela, preferencias, gustos, información familiar, grupos de pertenencia, estrato social, opiniones). Los datos pueden ser luego empleados con el propósito de provocar daños o realizar estafas y secuestros, entre otras conductas delictivas. Mucha de esa información pudo haber sido cargada en Internet por los menores a través de blogs, etiquetando fotos o en sala de chats, pudiendo ser utilizada por otros para causarles daño sin que ellos lo sepan.

• Robo o suplantación de identidad

Tras la obtención de datos personales de niños, niñas y adolescentes, así como de otros integrantes de la familia, los menores pueden ser utilizados para sustraer una identidad de otros y, en consecuencia, efectuar acciones en nombre de otra persona. Dichas acciones pueden estar orientadas a ocasionar daños económicos (por ejemplo: la compra por Internet con los datos de pago de un tercero) o morales (por ejemplo: la participación en un foro identificándose como otra persona).

• Abuso emocional

Con el objeto de establecer una relación de confianza, personas inescrupulosas acercan a los menores material audiovisual con contenido violento, pornográfico o sexual, en forma distorsionada o simulada, usando dibujos animados u otro tipo de formato destinado a la comunicación infantil o adolescente. De este modo buscan reducir cualquier posible resistencia, atraer o generar una relación de confianza para luego cometer otros delitos. También podrían obtener cierta información con el fin de utilizarla después para extorsionar al menor y obligarlo a realizar determinadas acciones, comprometiendo así su integridad.

• Abuso sexual y/o violencia

Mediante el anonimato que brinda Internet, abusadores y pedófilos entablan relaciones virtuales con niños, niñas y adolescentes, para luego coordinar encuentros reales en los que podrían abusar sexualmente del menor o llevar a cabo otras acciones violentas.

• Exposición a material inadecuado o engañoso

Internet es una gran fuente de contenidos, de carácter irrestricto. Todo niño, niña o adolescente que navegue libremente puede quedar expuesto a material inapropiado para su edad y nivel de maduración, contrario a la idiosincrasia familiar u opuesto a la orientación con que su familia ha establecido abordar temas como drogadicción, racismo, sexualidad o religión. Ejemplos de estos contenidos se encuentran en sitios con lenguaje hostil e inapropiado, imágenes violentas, textos en los que se hace apología de las drogas, intención discriminatoria, pornografía, hábitos dañinos de alimentación, entre otros.

• Acoso entre pares usando las nuevas Tecnologías de la Información y Comunicación (TIC) o "cyberbulling"

La facilidad de acceso a la tecnología permite que pueda ser utilizada por los mismos niños para incomodar o atemorizar a otros menores (por ejemplo, mediante mensajes de texto –SMS- o correos electrónicos incesantes). Esto puede ocasionar daños o trastornos psicológicos en las víctimas, que merecen atención por parte de adultos, docentes y toda la comunidad.

• Infracción a leyes, normas o disposiciones

Copiar material protegido bajo derechos de autor sin la debida autorización o descargar archivos de las más variadas características (películas, software o música) es una práctica que, por desconocimiento o

descuido, puede comprometer a los menores y sus familias, llevándolos a situaciones con implicancias judiciales e inclusive a cometer delitos.

Además, la mayor parte de la información que encontramos en Internet y su presentación no tienen garantías de certeza, razón por la cual es importante realizar verificaciones sobre la fuente y buscar otras referencias sobre las consultas realizadas en la web.

Usos de las tecnologías

Estos son los casos más comunes de uso de las tecnologías ante los cuales recomendamos prestar atención, ya que pueden presentar uno o más de los riesgos explicados previamente:

1. Navegación en la web.
2. Uso de correo electrónico.
3. Uso de mensajería instantánea (chat).
4. Uso de blogs, fotologs, páginas personales y redes sociales.
5. Uso de redes para compartir contenidos. Redes P2P.
6. Juegos en Red.
7. Uso de celulares.

Adicionalmente se ha incluido un punto relativo al "Uso de contraseñas", que debe ser considerado especialmente ya que atraviesa todos los servicios que requieren de una identificación.

1- Navegación en la web

Como ya hemos dicho, Internet permite el acceso a la más variada calidad y cantidad de contenidos. En muchos casos, la puerta de acceso es simplemente un clic. Por ello aconsejamos establecer un "acuerdo familiar" sobre los contenidos permitidos por los padres

a los niños, niñas y adolescentes y los tiempos dedicados al uso de las tecnologías (Internet, videojuegos, celulares).

Existen muchas páginas donde se pide al usuario que deje sus datos personales (formularios) con distintos argumentos. Es una práctica habitual en los sitios de concursos, por ejemplo. En este sentido, se debe enseñar a los menores a preservar su privacidad, a no brindar información privada de ellos ni de sus familias a menos que tal requerimiento se encuentre supervisado por un adulto. En el caso de los concursos, los contratos que los acompañan exigen aceptación explícita, razón por la cual deben ser leídos minuciosamente.

La edad, el entorno familiar, el grupo de pertenencia u otros factores son variantes que deberían tenerse en cuenta para realizar ajustes especiales sobre el otorgamiento de permisos de acceso a cierto tipo de contenidos.

Es posible que, aun involuntariamente, los menores accedan a contenidos que exhiben una extrema violencia, un lenguaje inapropiado, escenas inconvenientes o que desarrollan ciertos temas inadecuadamente (xenofobia, sexualidad, hábitos alimenticios dañinos, adicciones, etc.).

Por esta razón es importante conocer los intereses de niños, niñas y adolescentes, y es aconsejable navegar con ellos para generar espacios de confianza y hablar de modo claro sobre las situaciones que se les pueden presentar.

Otra recomendación es no ingresar a los sitios haciendo clic en los enlaces que puedan aparecer en correos electrónicos, chats, foros u otras páginas, especialmente si no se confía en quien presenta el enlace. Ésta es una de las principales vías de compromiso de las computadoras, ya que puede ocurrir que al acceder se descargue código malicioso sin que el usuario lo advierta o que se ingrese en sitios fraudulentos, ilegítimos o dañinos.

Es importante informar a los niños, niñas y adolescentes en edad escolar sobre el derecho de propiedad de las obras en el uso de ciertos contenidos que pueden estar protegidos. Por ejemplo, enseñarles que no se debe copiar y pegar material de una obra cuyo autor tiene derechos reservados o descargar películas, imágenes, software o música con estas características. Del mismo modo, deben saber que existen espacios colaborativos en los que se promueve compartir contenidos. Todo dependerá del tipo de licencia de uso que posea tal contenido o espacio.

2- Uso de correo electrónico

Por seguridad y para proteger la información de las computadoras recomendamos enseñar a niños, niñas y adolescentes a desestimar correos no solicitados o provenientes de desconocidos, ya que a través de ellos pueden ingresar programas maliciosos que dañan o comprometen la PC sin que el usuario lo advierta. También, el spam puede contener imágenes y expresiones no aptas para ellos.

Como ya mencionamos en la sección de navegación web, tampoco se deben descargar adjuntos ni ingresar a los sitios haciendo clic en los enlaces que figuran en dichos correos no solicitados. Al hacerlo, se podría descargar un código malicioso sin siquiera notarlo o acceder a sitios fraudulentos, ilegítimos o dañinos.

Es importante destacar que los menores suelen ser especialmente vulnerables a los correos que apelan engañosamente a la solidaridad u otros temas similares, ya sea mediante sus contenidos o sus asuntos (subjects) que atraen su atención y son utilizados como señuelos.

Es recomendable como ejercicio de buenas prácticas:

• tener la precaución, al enviar correos electrónicos a varias personas, de usar la modalidad de copia oculta (CCO), a fin de preservar la privacidad de esos usuarios y evitar difundir sus direcciones electrónicas sin autorización de sus dueños;

• tener dos cuentas de correo electrónico: una para comunicarse con familiares y amigos y otra para registrarse en foros, juegos y redes sociales. De este modo es más simple identificar posibles correos no deseados, ya que muchos foros o suscripciones son utilizados para recolectar cuentas de correo válidas y luego enviar spam.

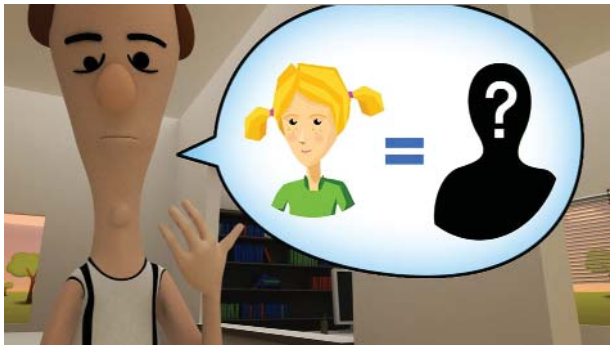
Como existe un mercado virtual en el que se compran y venden a precios considerables un conjunto de cuentas de correo electrónico, algunas personas originan y envían correos electrónicos con el fin de recopilar esas cuentas. La mayoría de los mensajes que piden ser reenviados a 5, 10 ó 15 personas suelen tener este objetivo. Generan así cadenas que parecen tener un mensaje generoso pero en verdad sólo persiguen el objetivo de obtener direcciones de correo válidas, para luego efectuar el envío de spam. Una recomendación importante es no reenviar este tipo de cadenas.

También circulan mensajes cuyos contenidos son falsos, bromas o engaños denominados "hoax" o "scam", y buscan despertar curiosidad, alarmar con distintos objetivos o, en algunos casos, estafar al destinatario. Los "hoax" se originan para que la persona que los reciba realice alguna acción en particular o haga circular el mensaje; no buscan una estafa monetaria directa. Por el contrario, los correos electrónicos en los que nos comunican que hemos ganado un premio millonario, que nos han dejado una herencia o que determinada empresa nos regalará un producto, para lo cual sólo tenemos que hacer un pequeño depósito o un giro de dinero, constituyen un engaño destinado a estafar monetariamente a quien lo recibe. Se los denomina "scam".

3- Uso de mensajería instantánea. Chat (mensajería instantánea o salas públicas)

El chat es probablemente la herramienta más utilizada por los niños, niñas y adolescentes.

Es una vía de comunicación instantánea, simple y efectiva que ofrece muchas ventajas y conlleva algunos riesgos. La cuenta de correo electrónico utilizada para chatear y el apodo o nick no tienen por qué tener relación directa con una persona. Este hecho, que para



un adulto puede ser sencillo de comprender, no es tan simple para un niño, niña o adolescente y puede llegar a confundirlo.

Por ello, es importante explicar a los menores que la comunicación vía chat puede ser engañosa cuando la identidad de aquel con quien se chatea no puede ser verificada por otro medio. Se debe prestar especial atención a los encuentros pautados por este medio. Es aconsejable desalentar este tipo de citas y, en caso de realizarse, se recomienda que se concreten en lugares públicos, con un acompañante adulto y durante las horas del día.

Es importante también enseñarles a los niños, niñas y adolescentes que ante la menor incomodidad que perciban en una comunicación de este tipo deben hablarlo con un adulto de su confianza o cortar la comunicación inmediatamente.

4- Uso de Blogs, fotologs, foros, páginas personales y redes sociales

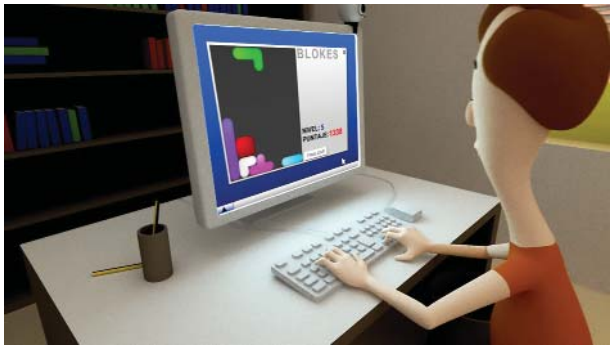
La información que se publica en este tipo de sitios puede estar a la vista de cualquiera. Sin embargo, muchos de estos portales tienen opciones para restringir los accesos sólo a contactos conocidos o sobre los cuales se tiene alguna referencia. Siempre se deben investigar estas funcionalidades y leer los términos de uso de cada servicio.

Algunos adolescentes son aficionados a volcar en estos sitios datos de su vida privada, como nombres y direcciones de familiares y amigos, datos de la escuela, teléfonos, toda su agenda, fotos o videos, haciéndolos completamente públicos y dejándolos a libre disposición. En este sentido, es importante advertirles que toda esta información puede ser utilizada con fines desconocidos.

Para esta instancia, como para otras, el acceso a los contenidos se realiza mediante un nombre de usuario y una contraseña, credenciales que permitirán agregar, eliminar o modificar datos. La preservación de estas credenciales o contraseñas, aspecto que trataremos más adelante, es un punto a tener en cuenta.

5- Uso de redes para compartir contenidos. Redes P2P

Se trata de la utilización de redes P2P (Peer to Peer) especialmente diseñadas para compartir contenidos de manera eficiente. Ejemplo de ellas son las aplicaciones como e-Mule, BitTorrent o Ares, utilizadas para compartir música, películas, software, libros y otros contenidos similares.



En estos casos los problemas pueden surgir a raíz de la búsqueda de contenido por medio de palabras clave, dado que es posible bajar archivos de estas redes que no siempre representan lo que el usuario realmente quería obtener. En ciertas ocasiones, es posible que se descarguen archivos de contenido inconveniente. También puede suceder que las descargas contengan código malicioso que puede infectar el equipo.

Finalmente, estas redes permiten bajar contenidos protegidos por la Ley de Propiedad Intelectual, violando lo dispuesto en esa norma. Es el caso de música, películas o programas propietarios.

6- Juegos en red

Muchos juegos tienen contenidos extremadamente violentos que deben ser objeto de atención por parte de padres y educadores.

Los juegos de simulación donde se desarrolla una vida virtual merecen especial atención, ya que al poder presentarse con un aspecto físico que simula el verdadero, el engaño puede articularse con mayor facilidad.

Hablar con los niños, niñas y adolescentes, conocer los entretenimientos preferidos y establecer tiempos dedicados a estas actividades resulta un buen medio de prevenir riesgos.

7- Uso de celulares

El celular tiene, cada vez con mayor frecuencia, la funcionalidad de una computadora: permite almacenar mucha información y acceder a funciones como pago de servicios, envío de correo electrónico, navegación web, correo electrónico y descarga de contenidos (textos, imágenes, videos y archivos en general). Con el

crecimiento de las aplicaciones para estos dispositivos, es esperable que los riesgos también vayan en aumento.

Aunque no son los más difundidos, existen muchos virus diseñados para celulares.

Adicionalmente aconsejamos tener cuidado cuando alguien pide prestado el celular, ya que se han registrado algunos casos en los que, por medio de una excusa convincente para obtenerlo, se han realizado maniobras fraudulentas.

Las posibilidades de capturar imágenes y videos de buena calidad a través de un celular, para publicarlos inmediatamente en Internet, ya es un hecho desde hace tiempo. Por este motivo, es importante que todos sepan que la imagen de una persona no debería publicarse sin su autorización.

En cuanto a la información almacenada, debemos tener presente que, aunque no se trate de un tema específico de seguridad informática, existe la posibilidad de robo físico del teléfono. Por ello, aconsejamos no almacenar información crítica o sensible (imágenes o videos privados), o hacerlo sólo cuando se los pueda proteger adecuadamente, como por ejemplo con clave. Nunca está de más mantener un resguardo alternativo o copia de la información almacenada.

Uso de contraseñas

Se debe instruir a los menores sobre buenas prácticas en el uso de las contraseñas, especialmente cuando se accede a Internet fuera del hogar, para evitar ser observados por terceros al momento del tipeo. Asimismo, es importante no anotarlas en papeles ni utilizar la opción de los navegadores para "recordar contraseña". En ningún caso las contraseñas deben compartirse con terceros ni ser enviadas por correo.

La adecuada construcción de las contraseñas es una barrera efectiva para evitar que otra persona logre acceder a nuestro espacio privado, sea éste una cuenta de correo, un perfil en una red social o una cuenta bancaria.

Por eso enfatizamos la recomendación de no utilizar contraseñas fáciles de adivinar (débiles) como nombres de familiares, mascotas, personajes conocidos o programas de televisión.

Otra recomendación se vincula con la extensión de las contraseñas, ya que cuanto más cortas sean, más fácil será su deducción. Por ello sugerimos emplear, como mínimo, 8 caracteres y tener la precaución de cambiarla periódicamente. Finalmente, si se sospecha del compromiso de una contraseña, es decir que alguien más la conoce, se la deberá reemplazar.

¿Qué puede pasar si la computadora tiene virus?

Aunque genéricamente se conozcan como virus, técnicamente sería más adecuado hablar de códigos o programas maliciosos, "malware" en inglés, término más amplio que comprende a un conjunto de instrucciones destinadas a infiltrar y causar daños más o menos graves en sistemas informáticos.

Un equipo comprometido por algún tipo de estos programas maliciosos implica grandes riesgos. La apertura de ventanas con incómodos contenidos, sistemas notablemente más lentos, pantallas con errores de sistemas, pueden ser síntomas de la presencia de "malware" o cuestiones más graves, como pueden ser el robo de información o la captura del equipo para formar parte de una "botnet".

Un equipo que ha sido capturado para formar parte de una "botnet" pudo haberse contaminado con sólo visitar un sitio diseñado para tal fin. En estos casos, sin que el usuario lo advierta, el control del equipo

es compartido con alguien más que puede utilizarlo, junto a un grupo de otros equipos, para atacar a un portal específico, para capturar todos los usuarios y contraseñas que se ingresen al equipo (inclusive los de la banca en línea) o enviar spam, entre otros fines fraudulentos.

La mayoría de estos ataques puede ser minimizado si mantenemos nuestros equipos con sistemas operativos y aplicaciones con todas las actualizaciones de seguridad (programas de oficina, juegos, navegadores, etc.), si somos cuidadosos con los contenidos de nuestro correo, al navegar, si evitamos hacer clic en enlaces sospechosos, si mantenemos un programa antivirus actualizado y lo ejecutamos periódicamente y si consultamos con un técnico especializado cuando notamos actividad anormal en nuestros equipos.

También son útiles otro tipo de herramientas como los "firewalls", cuya función es controlar las conexiones de nuestro equipo con el exterior, solicitando aprobación del usuario para permitirlas.

Recomendaciones para padres

• Usar las tecnologías y navegar por Internet experimentando y aprendiendo poco a poco cuáles son sus posibilidades, servicios y funciones, ya que son un excelente modo de comprender mejor este mundo, facilitando el diálogo con sus hijos.

• Conocer los intereses de los niños, niñas y adolescentes en Internet y compartir con ellos tiempo de navegación, especialmente con los más pequeños.

• Generar espacios de confianza para que los niños puedan comentar dudas o situaciones que les parezcan extrañas o incómodas.

• Colocar la computadora en un lugar público de la casa para que resulte más fácil observar las actividades de los menores en Internet.

• Evitar que los niños, niñas y adolescentes utilicen Internet durante la noche o durante períodos prolongados.

• Utilizar las funciones de control de contenido. Muchos sitios que incluyen contenido generado por los usuarios cuentan con funciones que permiten controlar el acceso a sus espacios. Asimismo, los proveedores de Internet ofrecen herramientas de "control parental" que los adultos pueden implementar fácilmente para proteger a sus hijos en la navegación.

• Hablar con los menores sobre los contenidos inadecuados con los cuales pueden encontrarse en Internet, como violencia, sexualidad, adicciones, etc.

• Elegir un sitio adecuado para sus hijos como página de inicio.

• Evaluar cualquier sitio desde donde los niños puedan acceder a Internet fuera de sus hogares con el objeto de garantizar su seguridad. Las medidas de control deberían ser similares a las establecidas en el hogar.

• Conocer los contactos con los que se comunican los menores y advertirles sobre los riesgos vinculados a la suplantación o robo de identidad.

• Analizar el uso de programas especiales que permiten supervisar las conversaciones de niños, niñas y adolescentes, aun cuando sea necesaria una revisión posterior con acuerdo o a pedido de ellos.

Enséñeles a sus hijos:

• A no intercambiar información personal, contraseñas o datos de la familia con desconocidos, ni subirlos o publicarlos en sitios públicos.

• A navegar en Internet de forma segura, respetuosa y responsable. Es imposible que pueda observar la actividad de sus hijos en la red en todo momento. Por eso, a medida que se hacen mayores, es necesario que aprendan a utilizar Internet de forma segura y responsable cuando están solos.

• A discernir qué hacer cuando se encuentren frente a contenido inconveniente.

• A respetar la privacidad de amigos, conocidos y familiares, no identificando a las personas que aparecen en sus fotos o perfiles públicos sin la correspondiente autorización, y a hacerse respetar cuando se sientan incómodos con alguna referencia a ellos en algún sitio, solicitando su eliminación de ser posible.

• A no aceptar a desconocidos como amigos en las "redes sociales" y contactos en el chat sin consultar si tienen amigos en común e interiorizarse de quiénes son. Hable de los riesgos con ellos.

• A no revelar ni compartir sus contraseñas.

• A no elegir la opción "recordar la contraseña" cuando se utilizan computadoras en lugares públicos como cíber, escuela o biblioteca escolar.

• A evitar realizar encuentros personales con gente que han conocido en la red sin la supervisión de un adulto de confianza.

• A comunicarse de forma responsable. Una buena norma de conducta podría ser: "Si tenés pudor o vergüenza de decir algo a la cara, no lo envíes por correo electrónico, chat o SMS, ni lo cuelgues en una página web".

• A comunicarse de manera respetuosa. Se debe tener siempre presente que detrás de un alias o nick se encuentra una persona y se deben seguir las mismas reglas de educación y respeto que garantizan la convivencia en la vida real.

• A comprender en qué consiste la privacidad. Se debe transmitir la importancia de proteger sus datos personales con ejemplos de la vida cotidiana para que comprendan que esa información puede ser utilizada en su contra.

Esté atento a lo que sus hijos hacen en Internet. Escúchelos y acompáñelos en esta etapa de descubrimiento.

Cuidados para toda la familia

Resumiendo, y desde el punto de vista técnico, es importante destacar que existe una variedad de herramientas para mitigar los riesgos descriptos.

Los filtros (programas o configuraciones) que permiten restringir el acceso a sitios, omitiendo el contenido que la familia ha considerado inconveniente, son gran utilidad, así como el software para monitorear o controlar los sitios visitados.

En general, estos programas denominados de "control parental" están disponibles para los navegadores más conocidos o pue-

den existir como aplicaciones separadas. Su finalidad es supervisar el uso que hacen los menores de Internet. Estos controles podrían suponer una intromisión en la intimidad de los menores, razón por la cual, a partir de cierta edad, se recomienda consensuar con ellos su aplicación.

Es importante también mantener la computadora adecuadamente protegida, esto es, manteniéndola libre de virus y cualquier código malicioso. Para ello se recomienda tener un producto antivirus actualizado, software original con todas las actualizaciones del proveedor y un firewall.

Decálogo de los e-derechos difundidos por la UNICEF para un uso didáctico y formativo de la red

• Derecho de acceso a la información y a la tecnología sin discriminación por motivo de sexo, edad, recursos económicos, nacionalidad, etnia, lugar de residencia, etc.

• Derecho a la libre expresión y asociación. A buscar, recibir y difundir informaciones e ideas de todo tipo por medio de la red. Estos derechos sólo podrán ser restringidos para garantizar la protección de los niños, niñas y adolecentes frente a informaciones y materiales perjudiciales para su bienestar, desarrollo e integridad, y para garantizar el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.

• Derecho de los niños, niñas y adolecentes a ser consultados y a dar su opinión cuando se apliquen leyes o normas a Internet que los afecten, como restricciones de contenidos, lucha contra los abusos, limitaciones de acceso, etc.

• Derecho a la protección contra la explotación, el comercio ilegal, los abusos y la violencia de todo tipo que se produzcan utilizando Internet.

• Derecho al desarrollo personal y a la educación, y a todas las oportunidades que las nuevas tecnologías como Internet puedan aportar para mejorar su formación.

• Derecho a la intimidad de las comunicaciones por medios electrónicos. Derecho a no proporcionar datos personales a través de la red, a preservar su identidad y su imagen de posibles usos ilícitos.

• Derecho al esparcimiento, al ocio, a la diversión y al juego también mediante Internet y otras nuevas tecnologías. Derecho a que los juegos y las propuestas de ocio en Internet no contengan violencia gra-

tuita ni mensajes racistas, sexistas o denigrantes, y respeten los derechos y la imagen de los niños, niñas y otras personas.

• Los padres y madres tendrán el derecho y la responsabilidad de orientar, educar y acordar con sus hijos e hijas un uso responsable de Internet: establecer tiempos de utilización, páginas que no se deben visitar o información que no deben proporcionar para protegerlos de mensajes y situaciones peligrosas, etc.

• Los gobiernos de los países desarrollados deben comprometerse a cooperar con otros países para facilitar el acceso de éstos y sus ciudadanos, y en especial de los niños, niñas y adolecentes, a Internet y a otras tecnologías de la información, para promover su desarrollo y evitar la creación de una nueva barrera entre los países ricos y los pobres.

• Derecho a beneficiarse y a utilizar en su favor la nuevas tecnologías para avanzar hacia un futuro más saludable, más pacífico, más solidario, más justo y más respetuoso con el medio ambiente, en el que se respeten los derechos de todos los niños, niñas y adolecentes.

Glosario básico de terminología informática

Botnet: colección de computadoras conectadas a Internet que interactúan entre sí para lograr la realización de cierta tarea de forma distribuida. Si bien ese conjunto de computadoras puede ser usado para aplicaciones útiles y constructivas, el término "botnet" se aplica, típicamente, a un sistema diseñado y utilizado para propósitos maliciosos. Dicho sistema está compuesto por equipos comprometidos que son introducidos en la "botnet" sin conocimiento de sus dueños. Los equipos comprometidos se conocen como "zombies" y al software malicioso que corre en ellos se lo denomina "bot".

Cyberbulling: también denominado e-Bullying, es el acoso cibernético entre pares. Es la utilización de herramientas de las nuevas tecnologías para el maltrato, agresión y atemorización de pares. En estos casos, quienes actúan violentamente contra los menores son otros menores. Aquí radica la importancia de considerar al niño, niña o adolescente no sólo en un rol pasivo o vulnerable en el que exclusivamente son los adultos quienes pueden violentar sus derechos, sino que ellos mismos también pueden ser sus propios agresores, abusadores o explotadores.

Firewall: cortafuegos en castellano. Es una parte de un sistema o una red diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo las comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar o descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Se utilizan para evitar que los usuarios de Internet no autorizados tengan acceso a redes o equipos privados conectados a Internet.

Grooming: acción de seducir a una persona menor de edad y así disminuir sus inhibiciones.

Hoax: mensajes fraudulentos que contienen información inexacta o falsa, que inducen al receptor a reenviar el mensaje a fin de difundir su contenido o a realizar acciones que, muy probablemente, le ocasionarán problemas. Muchas cadenas de correos electrónicos (los que "obligan" al destinatario a reenviarlo bajo pena de diversos males) se inician sólo con el fin de recolectar direcciones de correos. No pretenden ganancia económica directa. Se puede ver más información en el sitio www.rompecadenas.com.ar.

Ingeniería social: conjunto de técnicas de engaño que se aplican sobre las personas para obtener de ellas información de interés para el atacante, o para lograr que aquéllas efectúen alguna acción que éste persigue.

Malware: con este nombre se denominan genéricamente los programas que tienen un fin malicioso. Su expresión sinónima es "código malicioso".

Phishing: forma de engaño mediante la cual los atacantes envían un mensaje (anzuelo) a una o a varias personas con el propósito de convencerlas de que revelen sus datos personales. Generalmente esta información es utilizada luego para realizar acciones fraudulentas, como transferencias de fondos de su cuenta bancaria, compras con sus tarjetas de crédito u otros comportamientos delictivos que requieren el empleo de dichos datos.

Redes P2P: básicamente son denominadas así las redes donde el contenido se transfiere entre iguales. Todos los integrantes (equipos y usuarios) de una red ponen cierto material a disposición del resto y descargan lo que otros integrantes también ponen a disposición de los demás. Existen muchas de estas redes; de esa forma se optimizan las búsquedas. Cualquier nodo puede iniciar, detener o completar una transacción dentro de una red.

Scam: estafa en inglés. Correo electrónico (o página web) fraudulento que pretende estafar económicamente por medio del engaño. Generalmente se presenta como donación a recibir, lotería o premio al que se accede previo envío de dinero.

Spam: denominación del correo no deseado, enviado de manera masiva.

Bibliografía y referencias

• Búsquedas seguras en Google. Filtro SafeSearch (Búsqueda segura)

• Documento publicado por ArCERT sobre Botnet: www.jgm.gob.ar

• Espacio creado para brindar información a Jóvenes, Padres y Docentes sobre Seguridad en Internet. www.segu-kids.com.ar

• Folleto generado por la Policía Federal Argentina, División Delitos en Tecnologías y Análisis Criminal.

• Información Legislativa: http://infoleg.mecon.gov.ar

• Internet en Familia – Cómo orientar a los chicos cuando usan Internet. Ministerio de Educación - Escuela y Medios en conjunto con sectores privados.
www.jgm.gob.ar

• "Los chicos e Internet - Para una navegación responsable, provechosa y divertida". Portal educ.ar - Ministerio de Educación. www.educ.ar

• Manual del Instructor en Seguridad de la Información.
www.jgm.gob.ar

• Noticias y actualidad en la temática: http://chicosymedios.blogspot.com/

• Programa Internet Segura, por una navegación e interacción responsable. Asociación Civil "Chicos.net": www.chicos.net/ internetsegura/index.html

• Unicef: www.unicef.org/argentina/spanish/

Sitios recomendados

• Gobierno del Principado de Asturias. www.internetyfamilia.es

• Internet Segura - (Sitio con información sobre ciberbulling y ciberacoso): www.internetsegura2009.com/

• Portal de Microsoft en castellano "Proteja a su familia": http://www.microsoft.com/latam/protect/family/default.mspx

• Protégeles.com. www.protegeles.com/

• Todo lo necesario para que tus hijos naveguen seguros: www.protegeatushijos.com

• Sobre programas de control parental: www.protegeles.com

• Uso de contratos familiares para proteger a los niños en Internet:www.microsoft.com/spain/protect/family/guidelines/contract.mspx

Producción integral
Coordinación de Emergencias en Redes Teleinformáticas | **ArCERT**
Oficina Nacional de Tecnologías de Información | **ONTI**
Subsecretaría de Tecnologías de Gestión | **SsTG**
Secretaría de la Gestión Pública | **SGP**
Jefatura de Gabinete de Ministros | **JGM**

Ilustraciones - We Animate! www.weanimate.com.ar
Agradecemos la colaboración del Lic. Sergio Balardini
Noviembre 2009