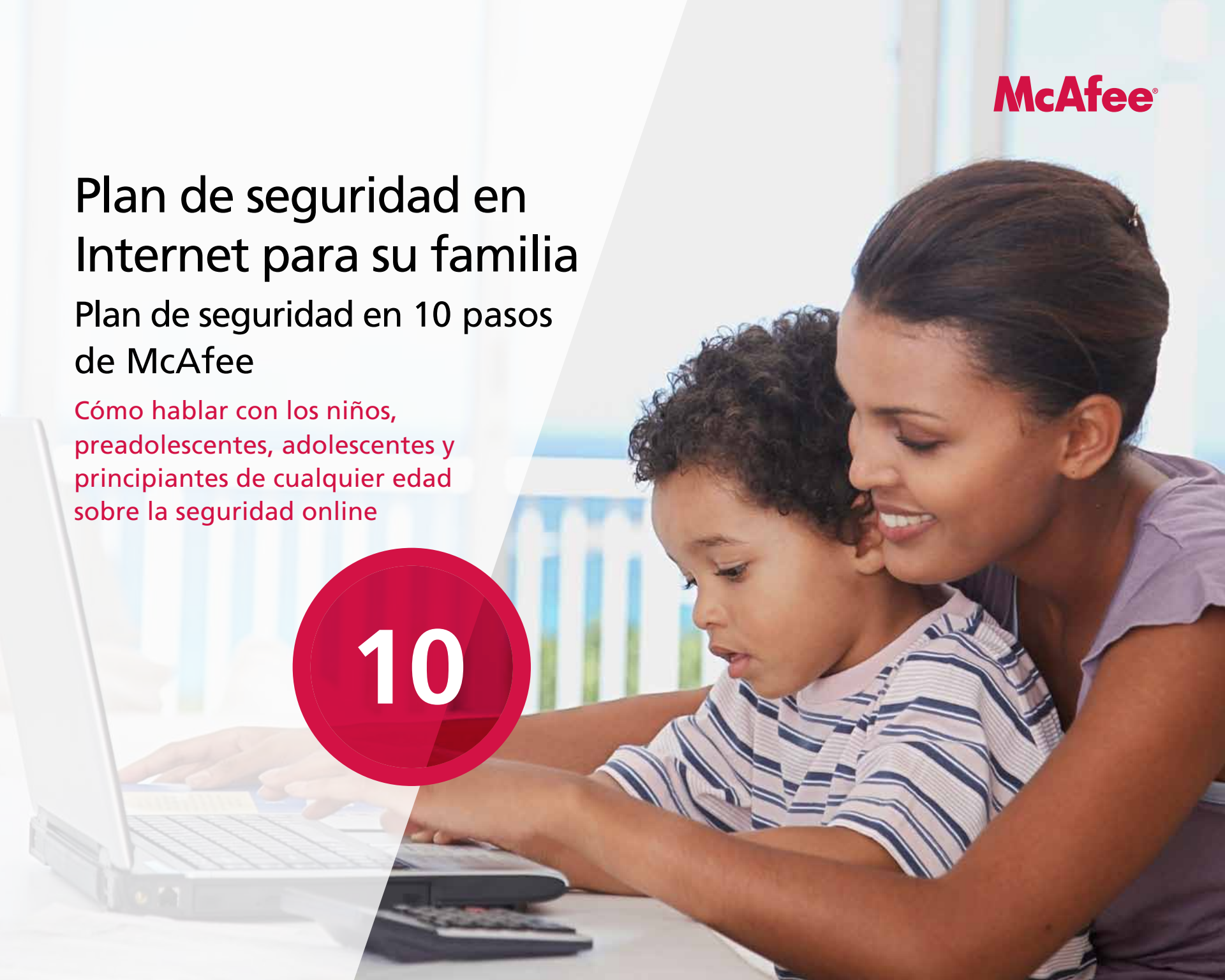
Plan de seguridad en Internet para su familia

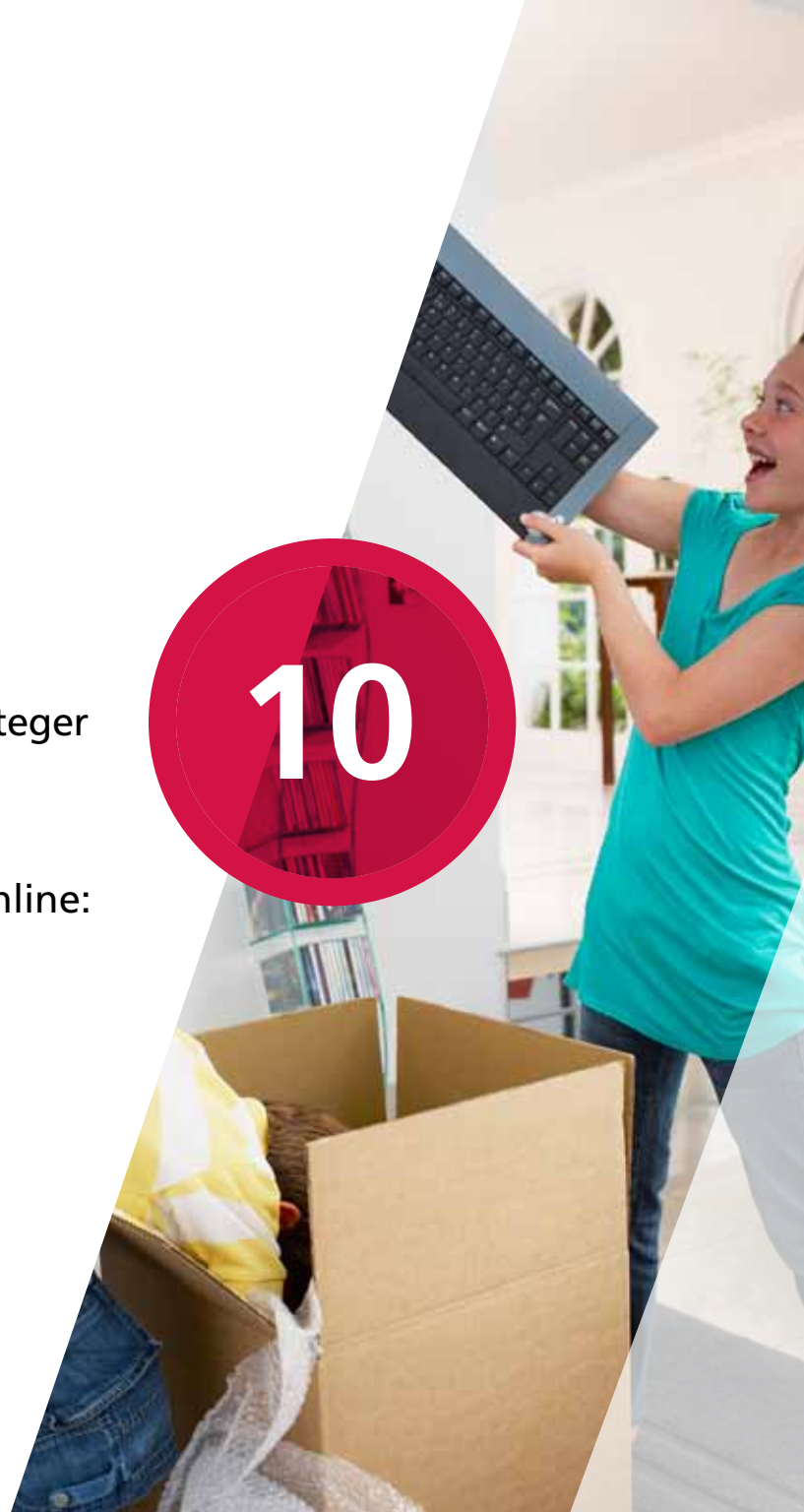
Plan de seguridad en 10 pasos de McAfee

Cómo hablar con los niños, preadolescentes, adolescentes y principiantes de cualquier edad sobre la seguridad online

10



Índice



Introducción

Millones de familias en todo el mundo utilizan Internet a diario para aprender, buscar, comprar, realizar operaciones bancarias, invertir, compartir fotografías, jugar, descargar películas y música, hablar con amigos, conocer gente nueva y participar en muchísimas otras actividades. Aunque el ciberespacio ofrece numerosas ventajas, oportunidades y posibilidades, también constituye un riesgo importante, ya que un gran número de nuevas amenazas aparecen todos los días.

No es de extrañar que los cibercriminales se aprovechen de Internet y de los usuarios que la utilizan. Tanto usted como los miembros de su familia necesitan estar protegidos cuando están online. Además de instalar un potente software de seguridad de una empresa de confianza para proteger a su familia de los piratas informáticos, ladrones de identidad, estafadores de correo electrónico y pederastas, es necesario seguir algunas reglas básicas de seguridad de Internet y utilizar el sentido común del mundo real. La solución ideal es un plan de seguridad de Internet para toda su familia.

Tan pronto como un miembro de la familia decida empezar a navegar, independientemente de su edad, es necesario educarlo sobre la seguridad cibernética. Debe ser consciente de que, aunque no disponga de un ordenador en casa, puede encontrar un equipo casi en cualquier lugar: en un colegio, una biblioteca, la casa de un amigo e incluso en el sótano de una iglesia. Es esencial que cualquier usuario conozca las reglas básicas sobre protección en el ciberespacio.

Internet hoy en día: actuar con precaución

- El 50% de los adolescentes han dado a conocer información personal en Internet.[1]
- Los hackers atacan equipos con acceso a Internet cada 39 segundos.[2]
- Según McAfee® Avert Labs®, existen 222.000 virus informáticos conocidos actualmente en la red y el número de amenazas aumenta cada día.
- El 30% de los adolescentes fueron víctimas de acoso cibernético una o más veces durante el período escolar.[3]
- Del 2007 al 2008, los delitos en Internet aumentaron en un 33%.[4]
- El 31% de los niños han estado expuestos a contenido perjudicial.[1]
- Aproximadamente 3,2 millones de personas en todo el mundo sufren anualmente estafas masivas de marketing online.[5]

1 EU Kids Online, Comparing children's online opportunities and risks across Europe (2006–2009)
2 Hackers Attack Every 39 Seconds – James Clark School of Engineering, Universidad de Maryland
3 theage.com.au
4 2008 Internet Crime Report, IC3
5 Autoridad Estratégica del Fraude Nacional (NFSA)

Plan de seguridad en 10 pasos para proteger a todos los miembros de su familia

Paso 1
Tener presente la ubicación del ordenador

En un hogar con niños, la ubicación del ordenador de la familia es una de las decisiones más importantes que se deben tomar. Le recomendamos que coloque el ordenador en una zona familiar con mucho movimiento y que limite el número de horas que los niños pueden utilizarlo. Asegúrese de disponer de software de seguridad para el ordenador con controles parentales, como los que puede encontrar en las soluciones de McAfee, o bien utilice software específico diseñado para proteger a los niños cuando están conectados, como McAfee Family Protection.

Paso 2
Trabajar en equipo para establecer límites

Decida exactamente lo que considera correcto o incorrecto respecto a:

- Los tipos de sitios web que se pueden visitar.
- Los foros y salones de charla en los que se puede participar:
  - Use sólo salones de conversación supervisados.
  - Asegúrese de que sus hijos eviten los salones de charla ".alt", que se centran en temas alternativos que pueden ser inadecuados para gente joven.
- Los temas que sus hijos pueden debatir online y el lenguaje que se considera inadecuado.

Paso 3
Acordar conjuntamente las reglas familiares para el uso del ordenador

Se recomienda lo siguiente:

- Nunca se registre con nombres de usuario que revelen su verdadera identidad o que puedan resultar provocativos.
- Nunca revele sus contraseñas.
- Nunca revele su dirección ni número de teléfono.
- Nunca publique información que revele su identidad.
- Nunca publique fotografías inadecuadas o que puedan revelar su identidad (por ejemplo: el nombre de una ciudad o un colegio serigrafiado en camisetas).
- Nunca comparta información con desconocidos que conozca en la red.
- Nunca se reúna cara a cara con desconocidos que conozca en Internet.
- Nunca abra archivos adjuntos procedentes de desconocidos.

Después de establecer las reglas, colóquelas al lado del ordenador.

Paso 4
Firmar un contrato sobre el comportamiento adecuado online

Redacte un contrato o utilice el que se muestra en la siguiente página para establecer las reglas entre todos los miembros de la familia sobre el uso adecuado del ordenador y el comportamiento correcto en Internet.

Compromiso de seguridad online

Dado que el uso de Internet y del ordenador es un privilegio que no quiero perder...

- Navegaré, realizaré búsquedas, trabajaré, jugaré y conversaré de forma segura mientras esté online.
- Seguiré todas las reglas que hemos acordado.
- No revelaré mi nombre verdadero, número de teléfono, dirección ni contraseñas a "amigos" virtuales.
- No concertaré una cita en persona con un usuario que haya conocido a través de la red.
- Si me encuentro en una situación insegura o incómoda, prometo informar (a mi padre, madre, tutor o profesor) para que puedan ayudarme.
- Prometo cumplir este compromiso y asumo que existen consecuencias respecto a las decisiones que adopte.

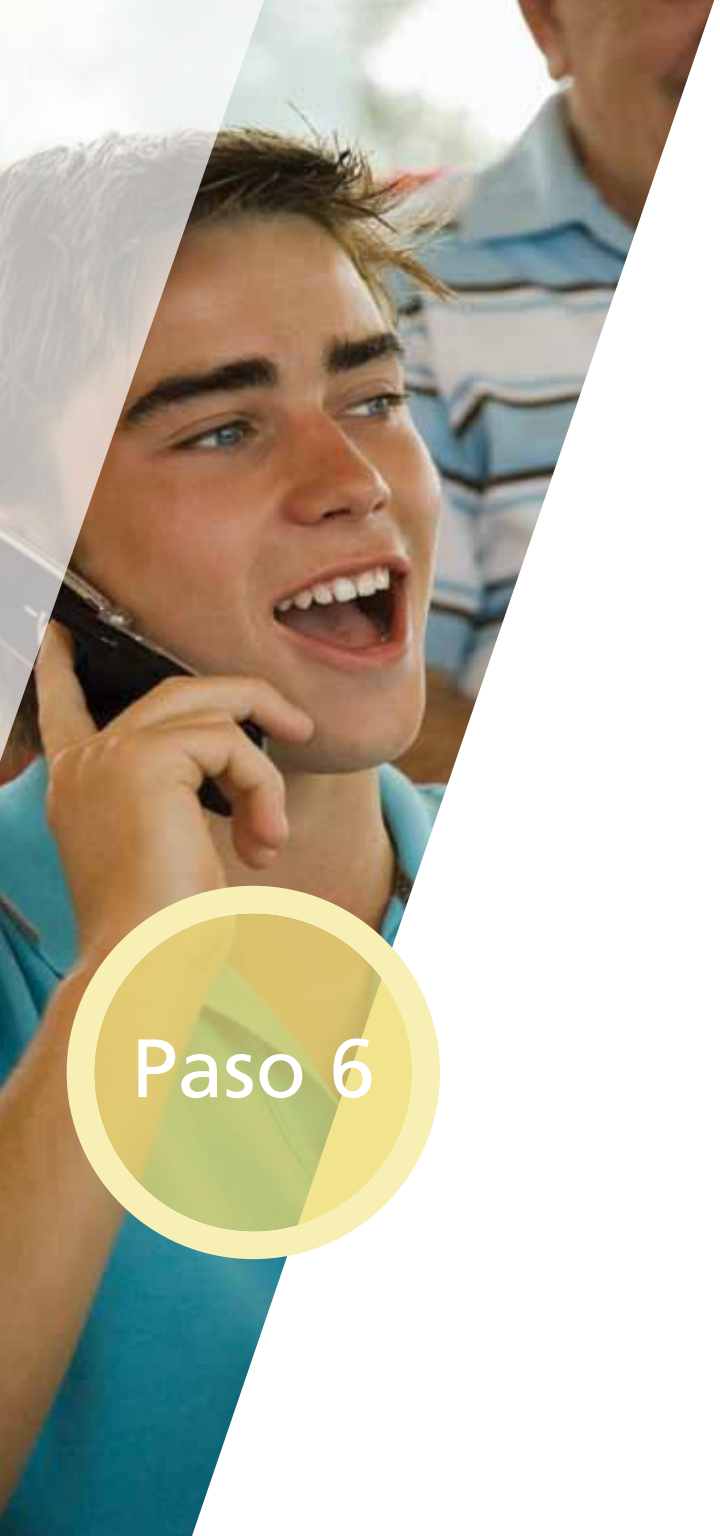
Firma del niño _____

- Como madre, padre, tutor o profesor, prometo estar a tu disposición cuando necesites ayuda y te ayudaré a resolver los problemas que puedan producirse de la mejor manera posible.

Firma del padre, madre, tutor o profesor _____

Paso 5
Instalar software

Asegúrese de disponer de un potente software de seguridad que proteja su ordenador de virus, hackers y spyware. También debe filtrar el contenido, las imágenes y los sitios web ofensivos. Este software debe actualizarse con frecuencia, ya que aparecen nuevas amenazas cada día. La solución ideal es un programa de seguridad que se actualice automáticamente, como el software con tecnología "Set-It-and-Forget-It" (Configurarlo y olvidarse) de McAfee.

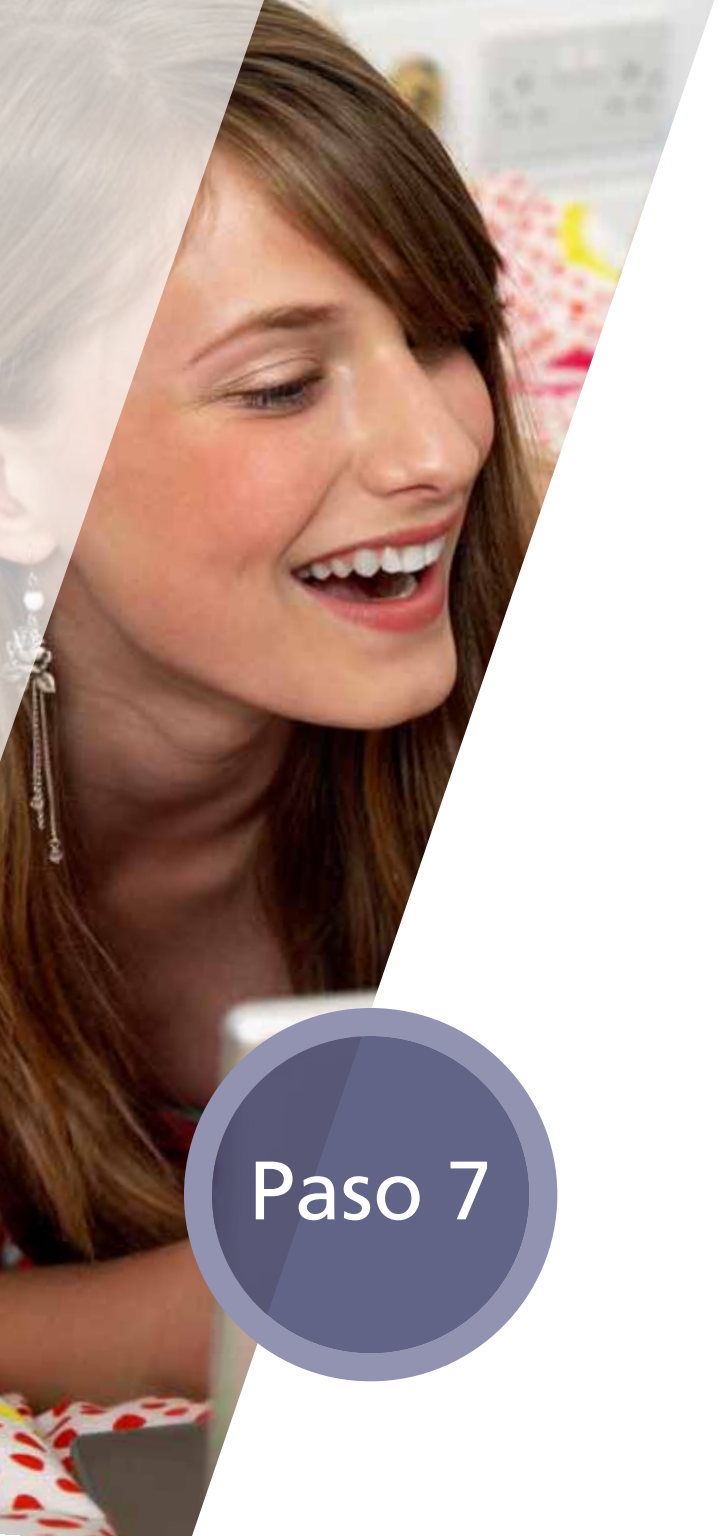


Paso 6
Utilizar controles parentales

Todos los proveedores de software de seguridad más importantes ofrecen controles parentales. Asegúrese de activarlos. Si está utilizando un programa de distribución libre o software sin controles parentales, contemple la posibilidad de adquirir software con estos controles. Invierta tiempo en aprender el funcionamiento de los controles y utilice las opciones que filtren o bloqueen material inadecuado.

Para proteger por completo a sus hijos cuando están conectados a Internet, utilice McAfee Family Protection además de los controles parentales del software de seguridad. El software McAfee Family Protection protege a los niños de todas las edades de la exposición a contenido inadecuado, los riesgos de las redes sociales, los desconocidos y otras amenazas online.

Por supuesto, estas herramientas tienen sus limitaciones. Ningún programa puede reemplazar a unos padres atentos y responsables que supervisen el uso que hacen sus hijos de Internet.



Paso 7

Recordar a los miembros de la familia que los usuarios que se conocen a través de la red son desconocidos

Cualquiera que se conecte debe comprender lo siguiente:

No importa la frecuencia con la que converse con sus "amigos" virtuales, ni el tiempo que lleve conversando con ellos ni el grado de familiaridad supuestamente adquirido entre las dos partes. Los usuarios que se conocen en Internet son desconocidos. Mentir es fácil, lo mismo que fingir la identidad de otra persona mientras se encuentra online. Especialmente los niños necesitan saber que un "amigo" nuevo puede ser en realidad un hombre de 40 años, y no alguien de su misma edad.

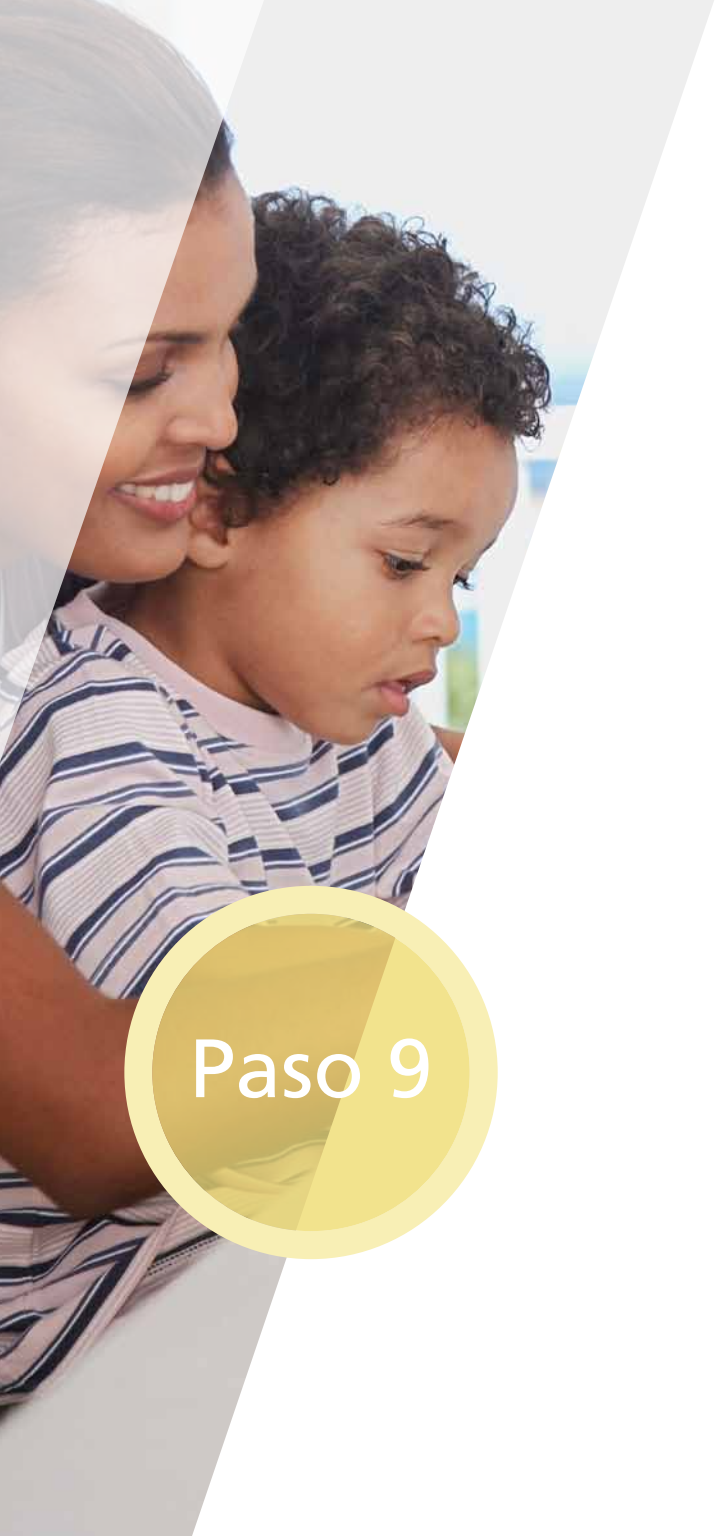
Los sitios web de redes sociales, como Bebo, Orkut y Facebook, son el lugar ideal para conocer gente nueva a través de la red. Por lo tanto, los padres deben visitar estos sitios y comprobar el perfil de sus hijos para asegurarse de que no generen conversaciones inapropiadas ni publiquen fotografías inadecuadas. Además, deben supervisar las conversaciones de mensajería instantánea de sus hijos para asegurarse de que no estén siendo perseguidos por un pederasta online.

Paso 8
Crear contraseñas difíciles

Para crear contraseñas difíciles de decodificar, utilice al menos 8 caracteres y, a continuación, una combinación de letras, números y símbolos. Las contraseñas deben cambiarse periódicamente para reducir la probabilidad de que una contraseña en particular se vea comprometida con el tiempo.

Técnicas de creación de contraseñas difíciles:

- Utilice una patente personalizada: “TMB717ARG”.
- Use varias palabras cortas con signos de puntuación: “la#chica^del@futuro”.
- Incluya el signo de puntuación en mitad de una palabra: “Beck%ham”.
- Haga uso de un método inusual de contraer una palabra: “peluqria”.
- Utilice la primera letra de cada palabra de una frase con un número al azar: “difícil decodificar esta contraseña” = “ddec2332”.
- No comparta sus contraseñas.



Paso 9
Comprobar el software de seguridad del ordenador

Abra el software de seguridad que está utilizando y compruebe que su ordenador esté protegido con las tres protecciones básicas siguientes: antivirus, antispyware y servidor de seguridad.

La seguridad de estas protecciones básicas debe verse incrementada con una aplicación contra propaganda y un software de búsqueda segura, como McAfee SiteAdvisor® que integra una protección contra fraude electrónico e índices de seguridad. Para las familias, es una idea excelente disponer de un conjunto de aplicaciones de protección en los equipos domésticos que también incluyan controles parentales, como el software McAfee Family Protection, y herramientas de prevención de robo de identidad.

Paso 10
Mantenerse informado

Cuanto más sepa acerca del tema, más seguros estarán su familia y su equipo. Visite el Centro de asesoramiento de seguridad de McAfee para obtener material educativo fácil de leer sobre la seguridad de Internet y de los ordenadores en: www.mcafee.com/advice.

Los principios básicos de la seguridad online

Para niños de 3 a 7 años

A

Hablar con los niños

Cuando hable con niños sobre la seguridad de Internet, hágalo con el ordenador apagado, de manera que pueda captar toda su atención. Comience explicándoles que un ordenador es una herramienta y que Internet es como una biblioteca electrónica gigante llena de información.

Explicar por qué es importante estar seguro en Internet, ya que el ordenador puede ser una puerta abierta a información personal importante. Cuénteles que gente mala puede apoderarse de su equipo y romperlo, por lo que deberían comprar uno nuevo.

Además, explíqueles por qué es importante no compartir información personal con otros usuarios online. Adviértales de que no deben utilizar sus nombres verdaderos ni contar dónde viven ni a qué colegio van.

B

Crear una lista especial de reglas para el ordenador que utilizan los niños

Esta lista debe incluir:

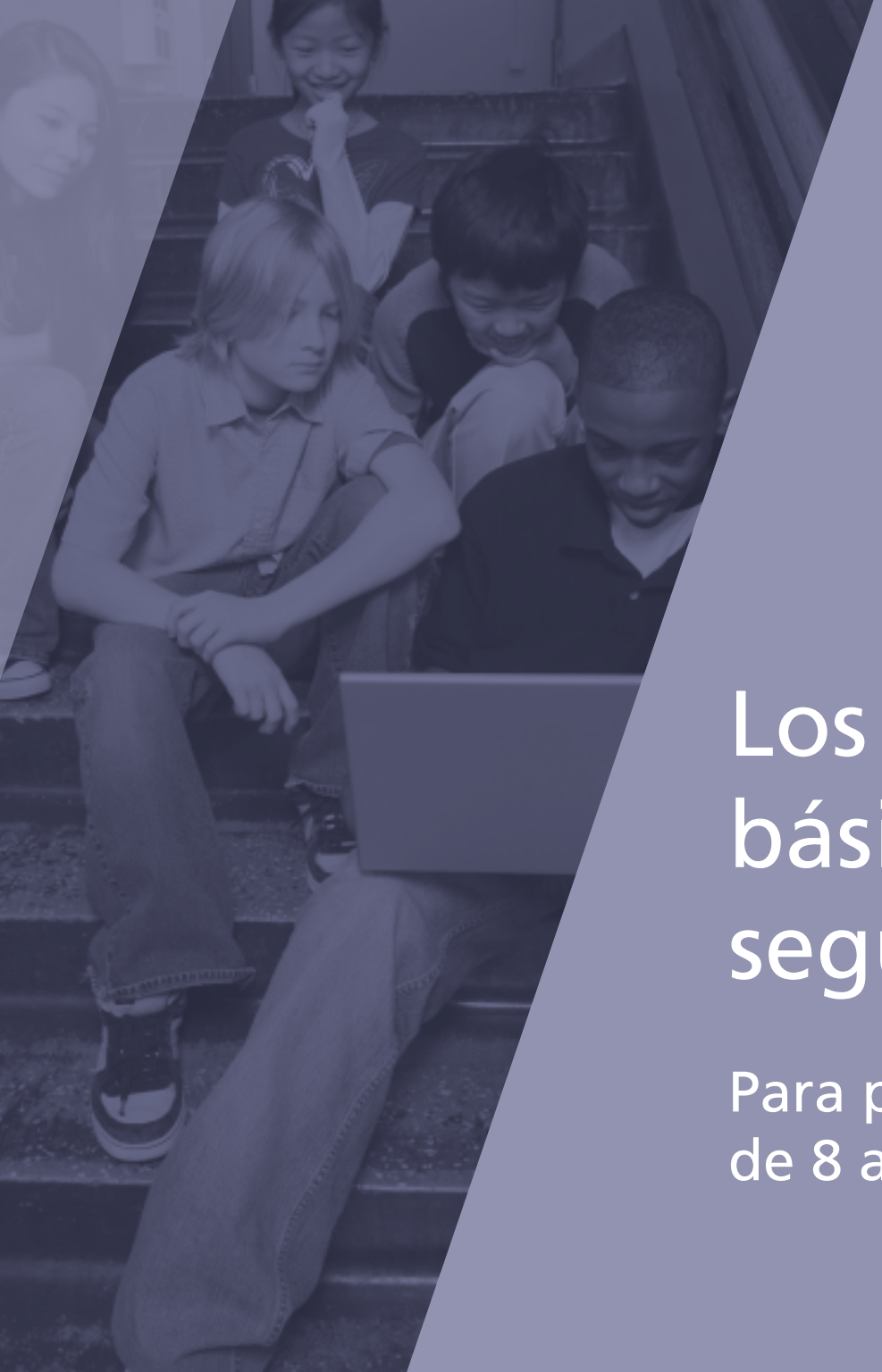
- No descargar música ni archivos de programa desde sitios Web sin el permiso de los padres.
- Usar sólo foros supervisados donde un adulto realmente controla la conversación.
- Nunca enviar una fotografía personal sin hablar primero con los padres.
- No utilizar un lenguaje incorrecto.
- No visitar sitios Web para adultos.
- Compartir información sólo con los usuarios conocidos en el mundo real, como compañeros de clase, amigos y familiares.
- No completar encuestas ni formularios online sin la ayuda de un adulto.
- Utilizar sólo motores de búsqueda especiales para niños, como Ask for Kids y Yahoo! Kids.

C

Utilizar navegadores y motores de búsqueda diseñados especialmente para niños

Asegúrese de que sus hijos usen navegadores y motores de búsqueda que no muestren palabras ni imágenes inadecuadas. Compruebe que estos navegadores incluyan filtros de palabras preestablecidos y sitios web seguros cargados previamente. Basta con revisar y dar el visto bueno a las palabras y los sitios web predeterminados.

Si sus hijos utilizan un motor de búsqueda estándar, asegúrese de activar los controles parentales en el motor de búsqueda para bloquear imágenes y contenido inadecuados de modo que no aparezcan en los resultados de las búsquedas.



Los principios básicos de la seguridad online

Para preadolescentes de 8 a 12 años

A

Hablar con los preadolescentes

Los niños preadolescentes entre 8 y 12 años son mucho más sofisticados de lo que solían ser años atrás. El término "preadolescente" fue acuñado para referirse exactamente a este grupo de niños que ya no se consideran "niños pequeños", pero que todavía no son "adolescentes". Sepa que los preadolescentes se sienten bastante cómodos con un ordenador, ya que han crecido con uno en casa o en el colegio.

Antes de hablar con los preadolescentes, es necesario tomar algunas decisiones de manera que pueda crear límites respecto al uso de Internet. Para informarles con claridad sobre estas reglas y su contenido, primero debe definirlas. Para ayudar a mantener la seguridad de sus hijos preadolescentes, debe conocer las respuestas a las siguientes preguntas:

- ¿El ordenador está en una zona pública de la casa?
- ¿Qué tipos de sitios Web son seguros como para que puedan visitarlos los preadolescentes?
- ¿Cuánto tiempo deben durar las sesiones online?
- ¿Qué pueden hacer mientras se encuentran conectados?
- ¿Con quién pueden interactuar?
- Si ha decidido no supervisar a sus hijos preadolescentes, ¿cuándo deben solicitar su ayuda y aprobación?

Una vez que conozca todas las respuestas a las preguntas anteriores, puede continuar con la charla. Con el equipo apagado, de manera que puedan captar toda su atención, debe explicar a sus hijos preadolescentes que un ordenador es una herramienta y que es importante estar seguro cuando se usa Internet.

Asegúrese de cubrir los siguientes puntos:

- Comentar sobre virus, spyware y hackers.
- Informar sobre cómo a los pederastas les gusta atraer a los niños hablándoles de sí mismos.
- Explicar por qué es importante estar seguro en Internet, ya que el ordenador puede ser una puerta abierta a información personal importante.
- Exponer cómo se producen los robos de identidad.
- Plantear el hecho de que usted o un experto informático (en caso de que usted no lo sea) puede supervisar cualquier acción realizada en el ordenador.
- Analizar cómo los criminales pueden apoderarse de su equipo y romperlo, por lo que deberían comprar uno nuevo.

B

Recordar a sus hijos que deben solicitar ayuda si se produce algo molesto en Internet

Durante la charla con sus hijos preadolescentes, haga hincapié en que deben informarle si reciben mensajes extraños o molestos mientras conversan online y que no se enfadarán con ellos ni les prohibirán que sigan usando Internet. Acláreles que entiende que ellos no pueden controlar los mensajes de otras personas y que no van a culparlos si esto sucede.

Además, asegúrese de que sus hijos preadolescentes no estén siendo víctimas de acoso escolar ni que estén acosando a otros niños online. Cuando los escolares dejan el colegio, no dejan necesariamente atrás a sus compañeros ni sus conflictos. Gracias a los ordenadores, los buscapersonas y los teléfonos móviles, los estudiantes pueden mantenerse en contacto en todo momento y pueden abusar de esta tecnología para molestar, acosar y dañar a otras personas.

C

Cómo bloquear usuarios y cómo informar sobre problemas

Si su hijo tiene un incidente en Internet mientras conversa, puede informar del problema y bloquear al usuario. Primero, copie los mensajes de la conversación y péguelos en un programa de procesamiento de textos. A continuación, envíe el registro copiado al moderador o administrador del foro. Puede encontrar la información de contacto del moderador o administrador en la sección de ayuda o informes del programa. La mayoría de los programas de conversación permiten bloquear a un usuario. Para ello, haga clic con el botón secundario del ratón en su nombre de la lista de contactos y seleccione la función “Bloquear” u “Omitir”.

Los principios básicos de la seguridad online

Para adolescentes de 13 a 19 años

A

Hablar con los adolescentes

De la misma manera que debe explicar a los adolescentes la importancia de la seguridad en la carretera antes de conducir un coche, también debe enseñarles la importancia de la seguridad de Internet antes de permitirles navegar a través de la red sin supervisión.

Una diferencia importante entre subirse a un coche y navegar por Internet es que no existen "reglas de carretera" reales en Internet. Esto lo convierte en un vehículo muy poderoso y peligroso a la vez. De esta manera, para evitar fallos en el ordenador, o incluso algo peor, debe establecer las reglas e imponer su cumplimiento. El objetivo es enseñar a los adolescentes que deben tener sentido común y apartarse de los peligros en Internet.

Explique a sus hijos adolescentes por qué es importante estar seguro en Internet.

Asegúrese de cubrir los siguientes puntos:

- Comentar sobre virus, spyware y hackers, y su funcionamiento.
- Informar sobre cómo a los pederastas les gusta atraer a gente joven vulnerable hablándoles de sí mismos.
- Explicar por qué es importante estar seguro en Internet, ya que el ordenador puede ser una puerta abierta a información personal importante.
- Exponer cómo se producen los robos de identidad.
- Plantear el hecho de que usted o un experto informático (en caso de que usted no lo sea) puede supervisar cualquier acción realizada en el ordenador.
- Analizar cómo los criminales pueden apoderarse de su equipo y romperlo, por lo que deberían comprar uno nuevo.

B

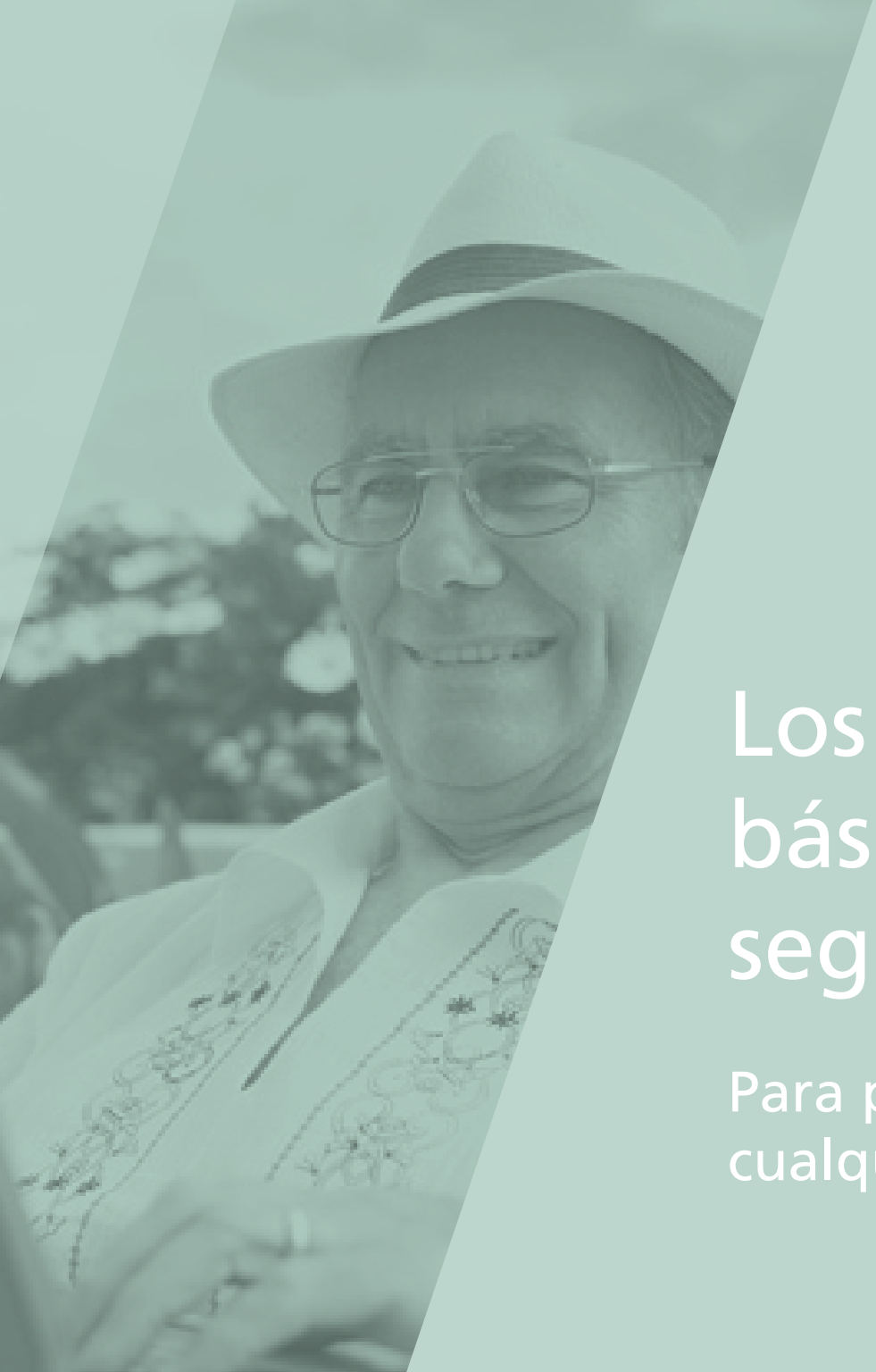
Recordar a sus hijos adolescentes que los usuarios que se conocen a través de la red son desconocidos

No importa la frecuencia con la que conversen con otros usuarios ni el grado de familiaridad supuestamente adquirido entre las dos partes. Los usuarios que los adolescentes conocen en Internet son desconocidos. La gente puede mentir sobre su identidad y el nuevo "amigo" de un adolescente puede ser en realidad un hombre de 40 años, y no alguien de su misma edad.

C

Comprobar los perfiles de sus hijos adolescentes en los sitios web de las redes sociales

Asegúrese de que sus hijos adolescentes no publiquen demasiada información personal en Bebo, Orkut o Facebook. Asegúrese también de que las fotografías que publiquen no sean provocativas. Recuérdeles que pueden suscitar el interés de los pederastas online, avergonzar a sus amigos y familiares, decepcionar a un posible representante de admisiones a la universidad o influenciar de forma negativa a un futuro empleador.



Los principios básicos de la seguridad online

Para principiantes de cualquier edad

Su cónyuge, su pareja, sus padres, sus familiares o sus abuelos pueden no estar familiarizados con el uso de un ordenador o de Internet. Puede que no tengan tanto conocimiento como creen, por lo que podrían ser víctimas de estafas online y ataques cibernéticos. Por lo tanto, necesitarán orientación de su parte. El debate sobre la seguridad de Internet debe incluir los siguientes puntos:

A

Virus, spyware y hackers

Si desea obtener definiciones sobre estos términos, podrá encontrarlas fácilmente a través de búsquedas online o en el glosario que podrá consultar en www.mcafee.com/advice

B

Peligros de robo de identidad y fraude electrónico

Un fraude electrónico ocurre cuando los criminales falsifican un sitio web y el correo electrónico de una empresa legítima e intentan robar contraseñas y números de tarjeta de crédito. Asegúrese de comprobar el estado de sus cuentas y de su tarjeta de crédito con regularidad.

C

Importancia de la precaución durante la descarga de elementos “gratuitos”

Recuerde a sus allegados el viejo axioma de que todo tiene un precio, aunque sea gratuito. Del mismo modo, avíseles que si descargan software, pueden instalarse programas publicitarios y spyware junto con la aplicación.

Más consejos sobre seguridad de Internet y equipos

Para obtener más información y consejos sobre seguridad de Internet y equipos, visite el Centro de asesoramiento de seguridad de McAfee en www.mcafee.com/advice

Información sobre McAfee

McAfee, Inc., con sede en Santa Clara, California, es la empresa dedicada a la tecnología de seguridad más importante del mundo. McAfee está continuamente comprometida a enfrentarse a los desafíos de seguridad más difíciles en todo el mundo. La empresa ofrece servicios y soluciones proactivas y probadas que ayudan a hacer más seguros los sistemas y las redes en todo el mundo, y permiten a los usuarios conectarse, navegar y comprar en Internet con mayor seguridad. Respaldada por un equipo de investigación galardonado, McAfee crea productos innovadores que ayudan a los usuarios, las empresas, el sector público y los proveedores de servicios al permitirles cumplir con las regulaciones, proteger datos, prevenir interrupciones, identificar vulnerabilidades, y controlar y mejorar continuamente la seguridad.

http://www.mcafee.com

McAfee, Inc. 3965 Freedom Circle, Santa Clara, California 95054 1.888.847.8766 www.mcafee.com

6385gde_10-step-internet-safety_intl_0509_es_fnl_Communicaid_Inc