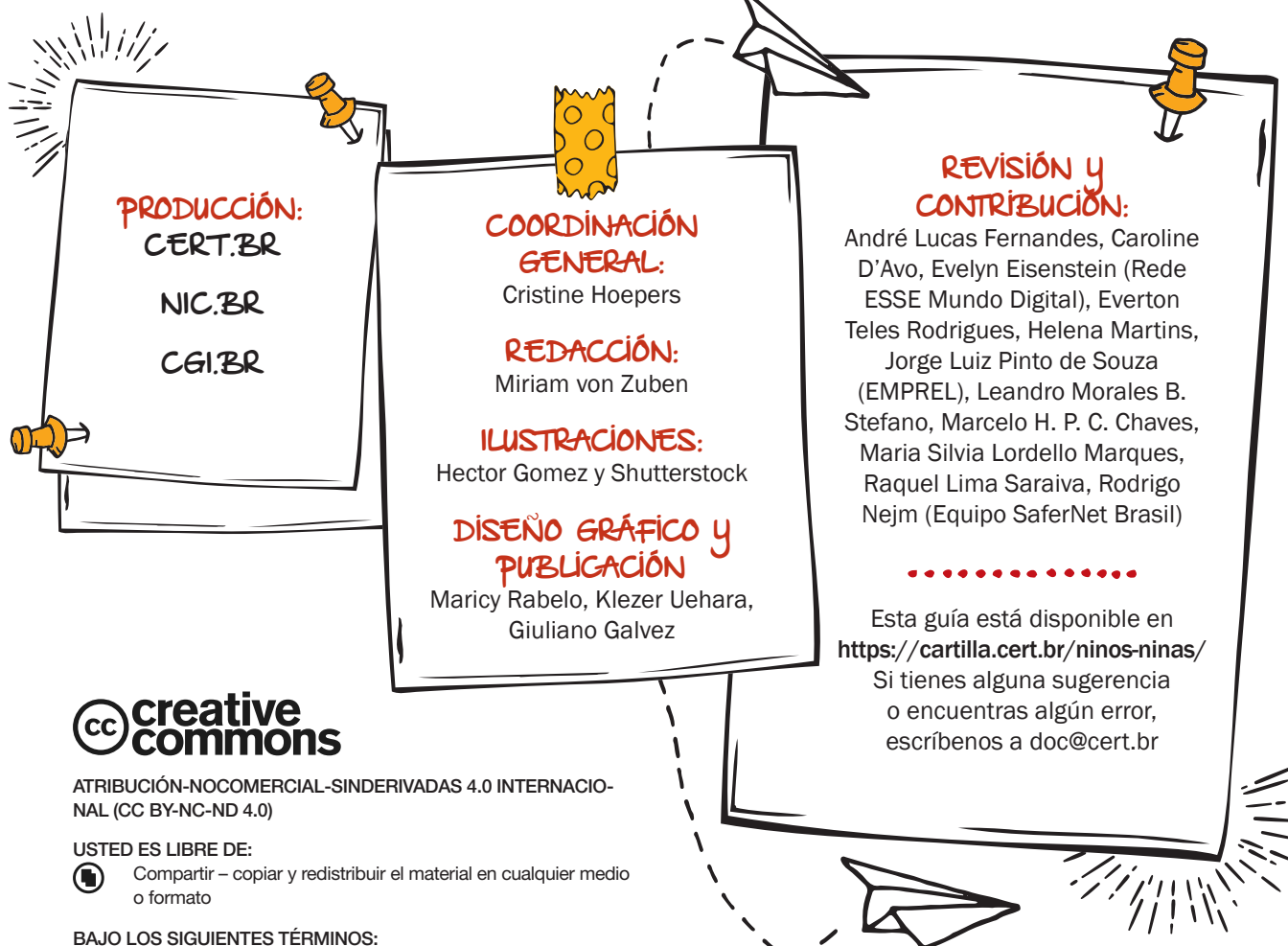




INTERNET SEGURA
PARA TUS HIJOS
2.ª EDICIÓN

¡TU PARTICIPACIÓN ES MUY IMPORTANTE!

cert.br nic.br cgi.br



PRODUCCIÓN:

CERT.BR

NIC.BR

CGI.BR

COORDINACIÓN GENERAL:

Cristine Hoepers

REDACCIÓN:

Miriam von Zuben

ILUSTRACIONES:

Hector Gomez y Shutterstock

DISEÑO GRÁFICO y PUBLICACIÓN

Maricy Rabelo, Klezer Uehara, Giuliano Galvez

REVISIÓN y CONTRIBUCIÓN:

André Lucas Fernandes, Caroline D'Avo, Evelyn Eisenstein (Rede ESSE Mundo Digital), Everton Teles Rodrigues, Helena Martins, Jorge Luiz Pinto de Souza (EMPREL), Leandro Morales B. Stefano, Marcelo H. P. C. Chaves, Maria Sílvia Lordello Marques, Raquel Lima Saraiva, Rodrigo Nejm (Equipo SaferNet Brasil)



Esta guía está disponible en <https://cartilla.cert.br/ninos-ninas/>
Si tienes alguna sugerencia o encuentras algún error, escríbenos a doc@cert.br



ATRIBUCIÓN-NOCOMERCIAL-SINDERIVADAS 4.0 INTERNACIONAL (CC BY-NC-ND 4.0)

USTED ES LIBRE DE:

Compartir – copiar y redistribuir el material en cualquier medio o formato

BAJO LOS SIGUIENTES TÉRMINOS:

ATRIBUCIÓN
Usted debe dar crédito de manera adecuada, brindar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que usted o su uso tienen el apoyo de la licenciante.

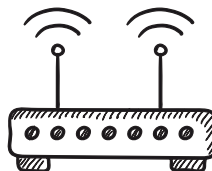
USO NO COMERCIAL
Usted no puede hacer uso del material con propósitos comerciales.

SIN DERIVADAS
Si remezcla, transforma o crea a partir del material, no podrá distribuir el material modificado.

<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>

HISTORIAL DE VERSIONES:

Febrero de 2017 - Primera edición
Octubre de 2022 - Segunda edición



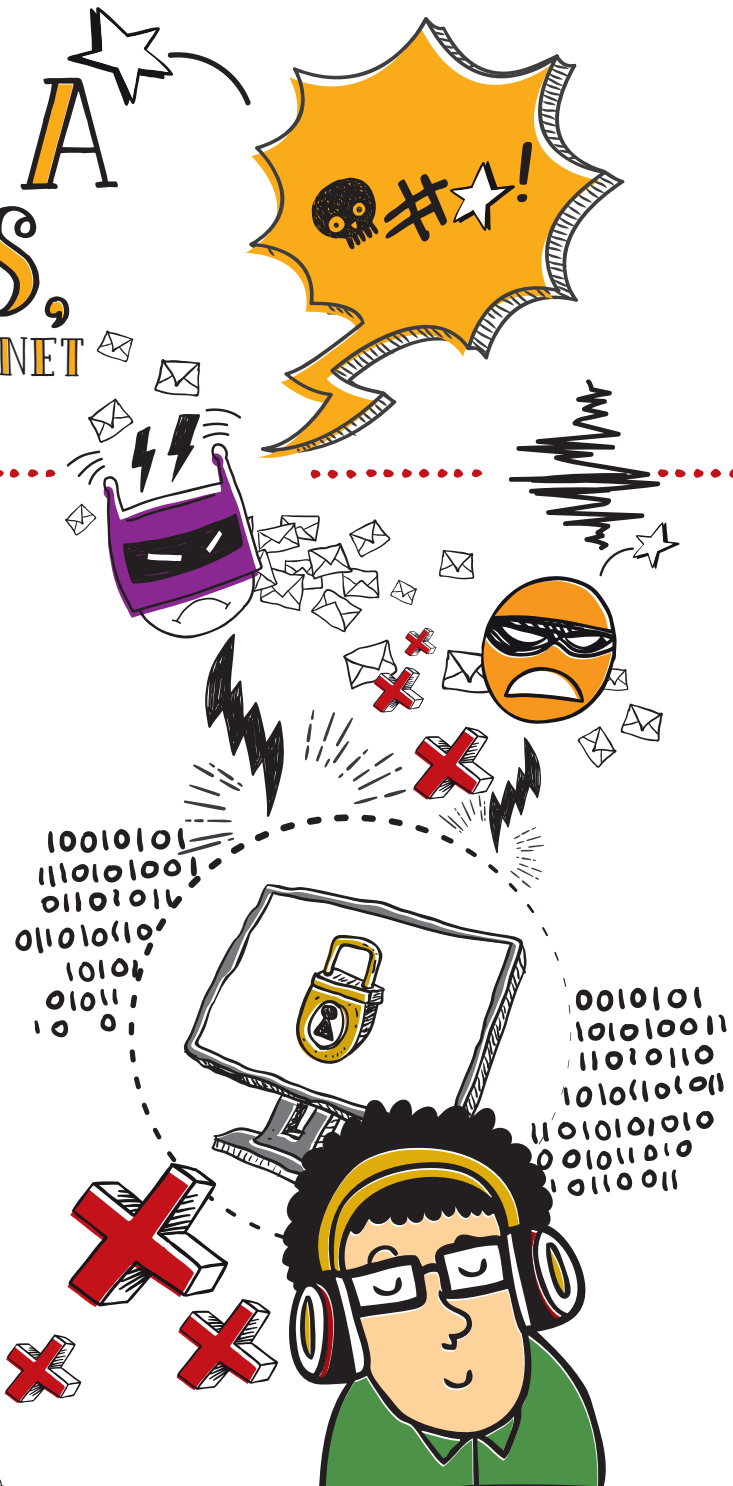
PROTEGE A TUS HIJOS, ENSÉÑALES A USAR INTERNET DE FORMA SEGURA

Así como orientas a tus hijos para que no hablen con extraños y miren a ambos lados de la calle antes de cruzarla, también debes advertirles sobre los peligros en Internet.

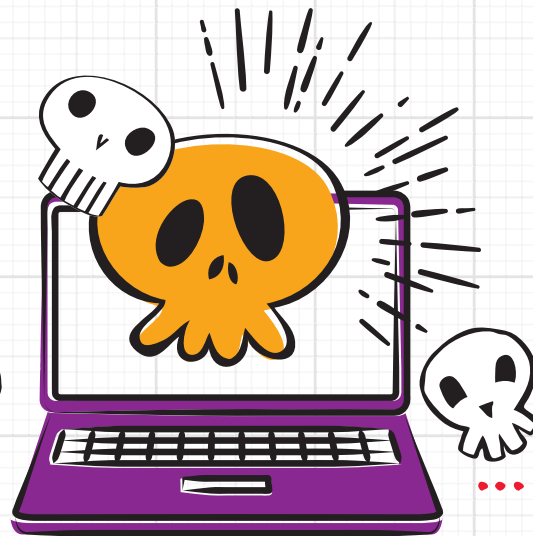
¿Cómo hacerlo? **LA MEJOR PREVENCIÓN ES LA INFORMACIÓN.** Si conocen los riesgos, tus hijos podrán evitarlos más fácilmente.

Con esto en mente, creamos la **GUÍA INTERNET SEGURA**, con consejos para que los niños y las niñas aprendan a protegerse de forma divertida. La guía está disponible en [HTTPS://CARTILLA.CERT.BR/NINOS-NINAS/](https://cartilla.cert.br/ninos-ninas/).

Creemos que la participación de la familia es fundamental en este proceso de aprendizaje. Por ello, también hemos creado esta guía complementaria con consejos y sugerencias para que ustedes —padres y tutores— puedan orientar a sus hijos para que utilicen Internet de una forma más segura.



CONOCE LOS RIESGOS



Internet tiene cualidades indiscutibles y bien conocidas. Cada día surgen nuevas posibilidades y todavía queda mucho por venir.

Sin dejar de reconocer todas las cosas buenas que Internet ofrece a tus hijos, es importante recordar que no tiene nada de virtual y presenta situaciones de riesgo ante las que debes prestar atención.



El uso excesivo de Internet

puede poner en riesgo la salud física y psicológica de tus hijos, disminuir su rendimiento escolar y afectar su vida social.




Al navegar por Internet, tus hijos pueden acceder a contenido inapropiado, falso, incompleto u ofensivo, como rumores, cadenas de mensajes, pornografía y violencia. Filtrar esta información requiere de sentido crítico y, dependiendo de la edad y madurez de tus hijos, puede que no estén preparados para ello.




Algunas personas se aprovechan de la falsa sensación de anonimato que da Internet para acercarse a los niños y cometer delitos como el *grooming*, el chantaje, la pornografía infantil y el secuestro.







La divulgación de información personal sobre tus hijos puede comprometer su privacidad, al igual que ellos pueden publicar información que comprometa la privacidad de sus familiares y amigos.




Las fotos y videos de tus hijos se pueden volver "virales" y, como consecuencia, ellos pueden convertirse rápidamente en "celebridades web", sus vidas pueden ser sobreexpuestas o incluso pueden ser ridiculizados.




Lo que se divulga en Internet se puede propagar rápidamente, pero es difícil de eliminar. Las fotos y videos de tus hijos pueden estar disponibles incluso después que sean adultos.



Tus hijos pueden ser víctimas de ciberacoso o acusados de esta práctica si publican, dan "me gusta" o comparten fotos, videos y mensajes que difamen y humillen a sus compañeros.



Los niños aún están en el período de formación de la personalidad, no tienen madurez emocional y no saben cómo lidiar con la opinión o el desprecio de los demás. Las imágenes publicadas de tus hijos pueden generar en ellos la expectativa de cómo serán recibidas y el no recibir "me gusta" o, incluso, recibir comentarios negativos puede causarles frustración.



Los dispositivos que usan tus hijos pueden infectarse con código malicioso (*malware*), lo que puede llevar a la pérdida de datos y el acceso no autorizado a la información personal.



NO SEAS TÚ EL VILLANO

ALGUNOS DE LOS RIESGOS QUE LOS NIÑOS ENCUENTRAN EN INTERNET SON CREADOS POR LA PROPIA FAMILIA QUE, EN GENERAL POR INGENUIDAD Y DESCONOCIMIENTO DE LOS PELIGROS, LOS EXPONE EXCESIVAMENTE.

¿ALGUNA VEZ HAS CREADO PERFILES EN NOMBRE DE TUS HIJOS?

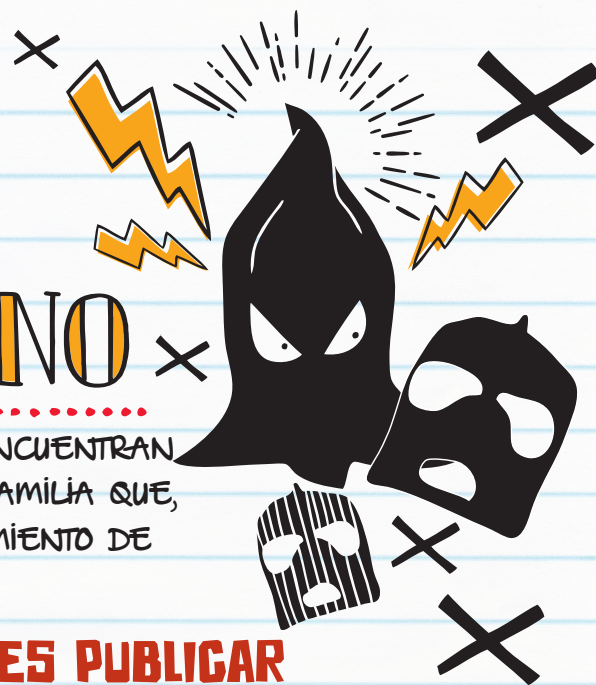
Algunos padres crean perfiles en nombre de sus hijos, publican sobre ellos e incluso interactúan como si los propios niños lo estuvieran haciendo. Algunos niños aún no han nacido pero ya tienen un perfil en las redes sociales. ¿Alguna vez has imaginado cómo se sentirán estos niños leyendo opiniones que no son las de ellos? En el futuro, ¿cómo se podrá diferenciar lo que ellos publicaron de lo que alguien más publicó en su nombre?

RECUERDA QUE ALGUNAS REDES SOCIALES EXIGEN UNA EDAD MÍNIMA PARA CREAR UNA CUENTA. Si los propios padres, que suelen ser el ejemplo para sus hijos, no obedecen las reglas, ¿cómo les van a reclamar luego a sus hijos?

¿SUELES PUBLICAR MENSAJES EN LAS REDES SOCIALES DE TUS HIJOS?

No es necesario publicar en los perfiles de tus hijos lo que es privado, propio de las relaciones familiares. Respeta su privacidad, individualidad e intimidad. El niño debe tener derecho a no querer ser expuesto y a construir su propio espacio en Internet a medida que madura su personalidad y su educación en el uso de las tecnologías.

Evita publicar mensajes llamándolos por apodos que solo usan entre ustedes o tratándolos de manera infantil. No los rezongues ni los regañes a través de las redes sociales. Habla con ellos antes de publicar cualquier foto o contenido familiar. **RECUERDA QUE INTERNET ES UN LUGAR PÚBLICO Y, COMO DICE EL REFRÁN, "LA ROPA SUCIA SE LAVA EN CASA".**





¿SUELES PUBLICAR FOTOS Y VIDEOS DE TUS HIJOS?

¿Alguna vez te has detenido a pensar hasta dónde llega tu derecho a exponer la privacidad de tus hijos? ¿Dónde comienza su derecho a no querer ser expuestos por sus padres? ¿A qué edad empiezan a tener derecho a su propia intimidad?

Lo que consideras “simpático” puede resultarles vergonzoso e incluso ser utilizado para hacerles *bullying*. Recuerda que el contexto familiar es privado.

Además, una foto de tus hijos desnudos o semidesnudos, dándose un baño o jugando en la playa puede parecerte inocente, pero esa misma foto puede ser utilizada por las redes de pedofilia para la explotación sexual comercial. Por lo tanto, **EVITA COMPARTIR FOTOS EN LAS QUE TUS HIJOS APAREZCAN CON POCAS ROPA.**

Exponer los hábitos de tus hijos (dónde estudian, qué cursos hacen, los lugares que frecuentan) puede ponerlos en riesgo de ser secuestrados. Se han denunciado diferentes casos de secuestro de menores, casos que se planificaron con información obtenida en las redes sociales. Por lo tanto, **EVITA PUBLICAR FOTOS QUE MUESTREN LA RUTINA DE TUS HIJOS.**

También existen los “secuestradores digitales”, que usan información real sobre los niños para crear perfiles falsos e interactuar con otras personas. En algunos casos, hasta comentan y comparten las fotos como si fueran los verdaderos padres del niño.

Para evitar esto, **TEN CUIDADO AL ACEPTAR EXTRAÑOS EN TUS REDES SOCIALES Y USA TU CONFIGURACIÓN DE PRIVACIDAD PARA LIMITAR QUIÉN PUEDE ACCEDER A TUS PUBLICACIONES.**





AYUDA A TUS HIJOS A PROTEGERSE



TU AYUDA ES MUY IMPORTANTE. DALES A TUS HIJOS ALGUNOS CONSEJOS PARA QUE USEN INTERNET DE FORMA MÁS SEGURA.



DA EL EJEMPLO

Los padres suelen ser la primera referencia para el comportamiento de los niños y es natural que copien sus hábitos y actitudes. **PERO DE NADA SIRVE DAR CONSEJOS SI LAS ACTITUDES NO SE CORRESPONDEN CON LO QUE SE DICE.**

¿Cómo pedirles a tus hijos un comportamiento que tú no tienes? Si comes mientras navegas por Internet, si siempre estás mirando las redes sociales mientras conversas, si nunca tienes tiempo para jugar pero encuentras tiempo para enviar mensajes que no son urgentes, tus hijos probablemente harán lo mismo.

ESTIMULA EL DIÁLOGO

No tiene sentido impedir que tus hijos accedan a Internet, ya que pueden hacerlo en secreto. Las prohibiciones muchas veces generan conflictos y dificultan el diálogo. Por lo tanto, mantente presente en el día a día, trata de hablar sobre las diferentes posibilidades que ofrece Internet y deja que tus hijos te cuenten sus experiencias.

Aprovecha también para aclarar dudas, porque así puedes indicar que hay un canal de diálogo abierto entre ustedes.

Al mostrar interés, será más fácil saber si necesita ayuda, si tiene algún problema o si algo le está molestando. **NAVEGAR CON TUS HIJOS PUEDE SER MUY DIVERTIDO Y EDUCATIVO.**

Trata de animarlos a compartir contigo cualquier experiencia desagradable. Para ello, intenta plantear situaciones hipotéticas, mencionar problemas que ya han ocurrido o aprovechar las oportunidades que se presentan, por ejemplo, casos que se han denunciado y que se están comentando. Esto les ayudará a entender los problemas y a ver las consecuencias, y les servirá de advertencia para que no pasen por las mismas situaciones o para que sepan cómo reaccionar.

RECUERDA QUE EL DIÁLOGO EDUCATIVO, ABIERTO Y FRANCO ES SIEMPRE LA MEJOR PROTECCIÓN QUE TUS HIJOS PUEDEN TENER FRENTE A LOS DESAFÍOS DE LA CONVIVENCIA EN SOCIEDAD.



REFUERZA EL CUIDADO QUE TUS HIJOS DEBEN TENER CON LOS EXTRAÑOS

No cabe duda de que Internet ayuda a acercar las personas que están lejos y a reforzar los lazos de amistad, pero también facilita el contacto con desconocidos de todo tipo. Algunos incluso pueden tener buenas intenciones, pero otros aprovechan la falsa sensación de anonimato que da Internet para intentar acercarse a los niños con fines criminales.

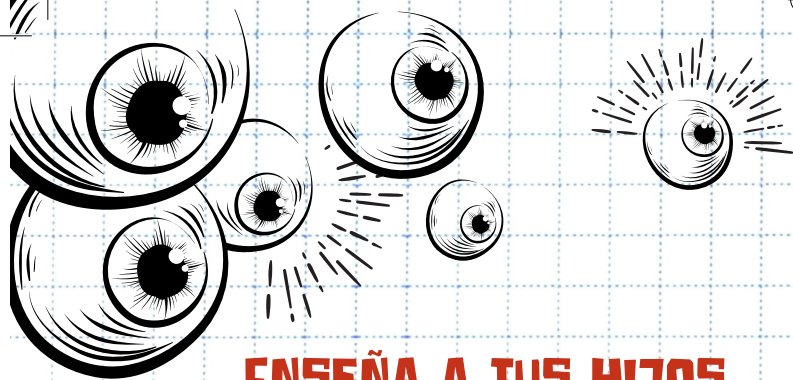
Desgraciadamente, muchos niños son engañados y terminan encontrándose en persona con desconocidos, con lo cual, sin darse cuenta, se exponen a grandes peligros. **ACONSEJA A TUS HIJOS QUE NUNCA QUEDEN DE ENCONTRARSE CON EXTRAÑOS O CON PERSONAS QUE SOLO CONOCEN POR INTERNET.**



OBSERVA EL COMPORTAMIENTO DE TUS HIJOS

Si tienes una computadora en casa, trata de mantenerla en un lugar donde, aunque sea desde lejos, puedas observar el comportamiento de tus hijos. Si acceden a Internet con equipos individuales, este tipo de supervisión se vuelve más complicado, pero aun así hay algunos indicios que pueden ser de ayuda.

Actitudes como minimizar o cerrar aplicaciones, cerrar con llave la puerta del dormitorio, bloquear el teléfono celular o la *tablet* y ponerse nervioso cuando te acercas pueden indicar que tus hijos están tratando de ocultar algo y posiblemente corriendo riesgos. Este es el momento de intentar hablar y entender lo que está pasando. Una relación de confianza es lo más importante. **HABLA Y ESCUCHA ANTES DE JUZGAR, PARA QUE ELLOS NO TENGAN MIEDO DE DENUNCIAR ALGO QUE LES MOLESTA.**



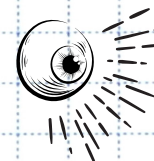
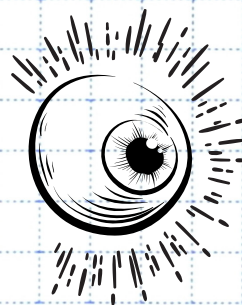
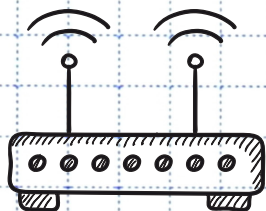
ENSEÑA A TUS HIJOS SOBRE LA PRIVACIDAD

Habla con tus hijos sobre la importancia de mantener la privacidad y de no compartir datos personales, como la dirección de su casa y la escuela a la que asisten.

CONSEJAJALES QUE SELECCIONEN SU CÍRCULO DE AMIGOS EN LAS REDES SOCIALES, SIN ACEPTAR A PERSONAS DESCONOCIDAS O POCO CERCANAS.

Ayúdalos a configurar su perfil para que las publicaciones sean privadas y solo sus amigos puedan acceder a ellas. Aún así, tus hijos deben saber que la red es pública y que no hay forma de controlar quién es el amigo del amigo del conocido... que también podrá ver y guardar lo que se publica y usarlo mañana o dentro de cinco años.

TAMBIÉN HABLA CON ELLOS SOBRE LA NECESIDAD DE PROTEGER LA PRIVACIDAD DE OTRAS PERSONAS, para lo cual no deben compartir información como dónde trabajan o las cosas que compraron, ni publicar sin autorización fotos o videos en los que aparecen otras personas.

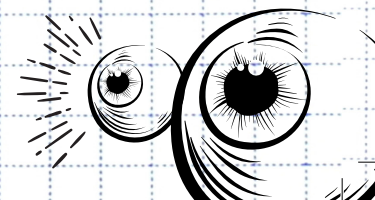


¿Y qué pasa con la privacidad de los niños? ¿Es apropiado que los padres tengan sus contraseñas y que controlen lo que hacen?

La respuesta a esta pregunta es bastante controvertida y particular. Cuando eras niño, probablemente no te gustaba que tocaran tus cosas o que escucharan tus conversaciones, pero por otro lado, es probable que la exposición a los riesgos no fuera tan alta como ahora.

Como te debe haber pasado a ti, la confianza de los padres se gana poco a poco. Dejar que tus hijos naveguen solos es como tener una llave de la casa: al principio, los padres se niegan a dársela, luego se la entregan pero con distintas recomendaciones, hasta que, finalmente, les entregan una copia y dejan de preocuparse.

Si bien al principio los niños necesitan una supervisión constante para realizar las tareas, con el tiempo y con orientación, se vuelven autónomos y pueden resolver las cosas por sí mismos. Cuándo y cómo ocurre esta transición depende del comportamiento de cada niño y de cada familia.





TEN CUIDADO CON EL CIBERACOSO

Las víctimas de *cyberbullying* o ciberacoso suelen mostrar síntomas como depresión, baja autoestima, ansiedad, agresividad, miedo y sentimientos negativos. También tienden a tener problemas en su rendimiento escolar y empiezan a evitar la escuela.

MANTENTE ALERTA SI TUS HIJOS MUESTRAN ESTAS SEÑALES E INTENTA AVERIGUAR EN LA ESCUELA SI ALGO ESTÁ SUCEDIENDO. Trata de hablar con ellos o anímalos a hablar con otras personas de tu confianza, como un hermano mayor, un tío, un primo o un maestro.

Si alguno de tus hijos comete ciberacoso, tú puedes ser considerado responsable por ser su representante legal.


ENSÉÑALES SOBRE LA IMPORTANCIA DE RESPETAR A LAS DEMÁS PERSONAS, que no debe compartir ni crear contenido humillante sobre sus compañeros y que las bromas tienen límites y pueden ofender. Pídeles que traten de ponerse en el lugar de la víctima y que piensen si les gustaría que les hicieran lo mismo.



PRESTA ATENCIÓN A LOS LÍMITES DE EDAD

Muchos sitios en Internet estipulan una edad mínima para sus usuarios. Por ejemplo, algunas redes sociales solo permiten usuarios mayores de 13 años de edad.

Los niños menores de la edad estipulada por los sitios que mienten sobre su edad para crear una cuenta se exponen a riesgos, como el contacto temprano con personas malintencionadas y el acceso a contenido considerado inadecuado para su franja etaria. Además, si sucediera algo malo, los padres podrían ser responsabilizados.




ESTABLECE REGLAS

Desde los primeros accesos, establece límites claros para el uso de Internet, por ejemplo, después de hacer los deberes, solo los fines de semana, unas horas al día y la hora límite para su uso.

TEN EN CUENTA QUE NO TIENE SENTIDO CREAR REGLAS DEMASIADO RÍGIDAS Y POCO REALISTAS, YA QUE ES IMPOSIBLE CONTROLARLAS TODO EL TIEMPO. Incluso si para hacer cumplir las reglas usas las funciones de control parental (de las que hablaremos más adelante), los niños pueden encontrar formas de eludirlas y no tendrán las mismas restricciones en otros dispositivos, como en la escuela o en la casa de un amigo.

Por lo tanto, es importante que las reglas se acuerden y justifiquen previamente, respetando las necesidades del niño y preservando su salud física y mental.



UTILIZA EL CONTROL PARENTAL

AUNQUE NADA REEMPLAZA EL DIÁLOGO Y LA MEDIACIÓN DE LOS PADRES, LA TECNOLOGÍA SE PUEDE USAR COMO UN ALIADO PARA AYUDAR A PROTEGER A LOS NIÑOS DE LOS RIESGOS DE INTERNET.

El control parental es un conjunto de funciones de seguridad disponibles en muchos sistemas operativos, sitios web y dispositivos como *routers* y consolas de juegos. También se puede instalar por medio de aplicaciones pagas o gratuitas.

Las funciones de control parental varían según la forma en que estén disponibles. Por ejemplo:



» **BUSCADORES:** permiten definir filtros de acuerdo con la calificación de edad del contenido.

» **SISTEMAS OPERATIVOS:** permiten restringir a qué sitios web pueden (o no pueden) acceder los niños, qué aplicaciones pueden ejecutar, con quién pueden comunicarse y establecer límites de tiempo, como el tiempo máximo de uso diario, la hora de dormir y reglas específicas para los días de semana y los fines de semana. También impiden el cambio de contraseñas y muestran el historial de actividades, entre ellas los sitios web visitados y las aplicaciones utilizadas.

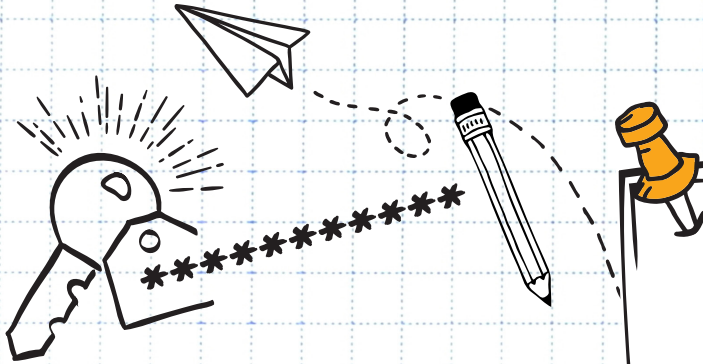
» **TIENDAS DEL SISTEMA OPERATIVO:** permiten definir la calificación (libre o por edad) de las aplicaciones que los niños pueden comprar, descargar e instalar, las películas que pueden ver, y los libros que pueden leer.

» **USUARIOS Y PERFILES RESTRINGIDOS:** permiten crear tipos de cuentas especiales donde las actividades son restringidas y están supervisadas.

» **SERVICIOS MEDIANTE CAMBIO DE DNS¹:**

permiten filtrar los sitios web a los que se accede, cambiando los servidores DNS configurados en los dispositivos que usan los niños o en el *router* de la red residencial. Estos servidores tienen reglas específicas para evitar el acceso a sitios maliciosos o restringidos a menores de 18 (por ejemplo, con contenido pornográfico).

¹ DNS (*Domain Name System*) significa sistema de nombres de dominio y, entre otras cosas, se encarga de traducir el nombre de las máquinas/dominios a la dirección IP correspondiente y viceversa.



Es importante que los niños no conozcan la contraseña de administración de los equipos ni la especificada en el servicio de control parental para que no puedan deshabilitar la protección.

A pesar de ser bastante útil, **EL CONTROL PARENTAL DEBE USARSE COMO UNA PROTECCIÓN ADICIONAL**, ya que puede tener fallas y no estar presente en todos los dispositivos y lugares desde donde los niños acceden a Internet, como la escuela o la casa de los amigos. Es por ello que un buen diálogo constante entre padres e hijos sigue siendo fundamental para ayudar a los niños a reconocer situaciones de riesgo y tratar de evitarlas.

LA MEJOR TECNOLOGÍA SIGUE SIENDO LA CONCIENCIA Y EL SENTIDO DE LA RESPONSABILIDAD. Ninguna característica de seguridad podrá desarrollar esta madurez y mucho menos reemplazar el sentido de autocuidado y autoprotección que requiere la vida en general, lo que incluye Internet, los juegos y las aplicaciones.



AYUDA A TUS HIJOS A PROTEGER LAS CUENTAS DE ACCESO

Explica a tus hijos la importancia de crear buenas contraseñas, evitando contraseñas fáciles de adivinar, como “123456”, “abcd”, “asdf”, su nombre, apellido, fecha de nacimiento, nombre de su perro o equipo favorito. Se recomienda que escojan contraseñas largas y que habiliten la verificación de dos pasos.

Enséñales a cerrar siempre la sesión de las cuentas de acceso cuando usen computadoras comunes o de otras personas, como en la casa de amigos, bibliotecas y escuelas, para que el próximo usuario no pueda acceder a ellas.


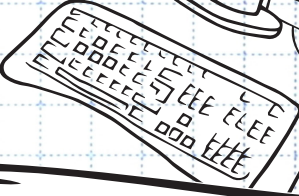

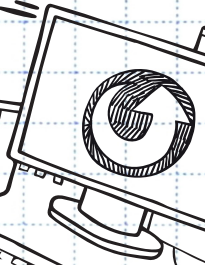



PROTEGE LOS DISPOSITIVOS QUE USAN TUS HIJOS




Los dispositivos que usan tus hijos pueden estar infectados por código malicioso (*malware*) que puede comprometer los datos almacenados, reducir su velocidad y hacer que dejen de funcionar. Por eso es importante que tomes algunas precauciones:

- » MANTÉN LOS DISPOSITIVOS SEGUROS, CON TODAS LAS ACTUALIZACIONES APLICADAS Y LAS APLICACIONES INSTALADAS CON LAS ÚLTIMAS VERSIONES.
- » INSTALA Y MANTÉN ACTUALIZADOS MECANISMOS DE SEGURIDAD, COMO UN ANTIVIRUS Y UN FIREWALL PERSONAL.



Algunos sistemas tienen funcionalidades que permiten ubicar el dispositivo a distancia y que, para funcionar, necesitan que el servicio de localización esté activado. Activar este servicio puede ser muy útil en caso de pérdida o robo del equipo, pero hay que tener cuidado.

Quando el servicio de localización está activado, otras aplicaciones, como las redes sociales, pueden acceder a la ubicación del niño y publicar esa información automáticamente. Algunos sistemas permiten configuraciones específicas por aplicación. Si eliges activar este servicio, verifica cuáles aplicaciones tendrán acceso a la ubicación de tus hijos y deshabilita las que no desees.



MANTENTE INFORMADO



En <https://cartilla.cert.br/ninos-ninas/>, además de este material, también encontrarás la guía creada especialmente para tus hijos.

Consulta también la Cartilla de Seguridad para Internet.



<https://cartilla.cert.br/>

