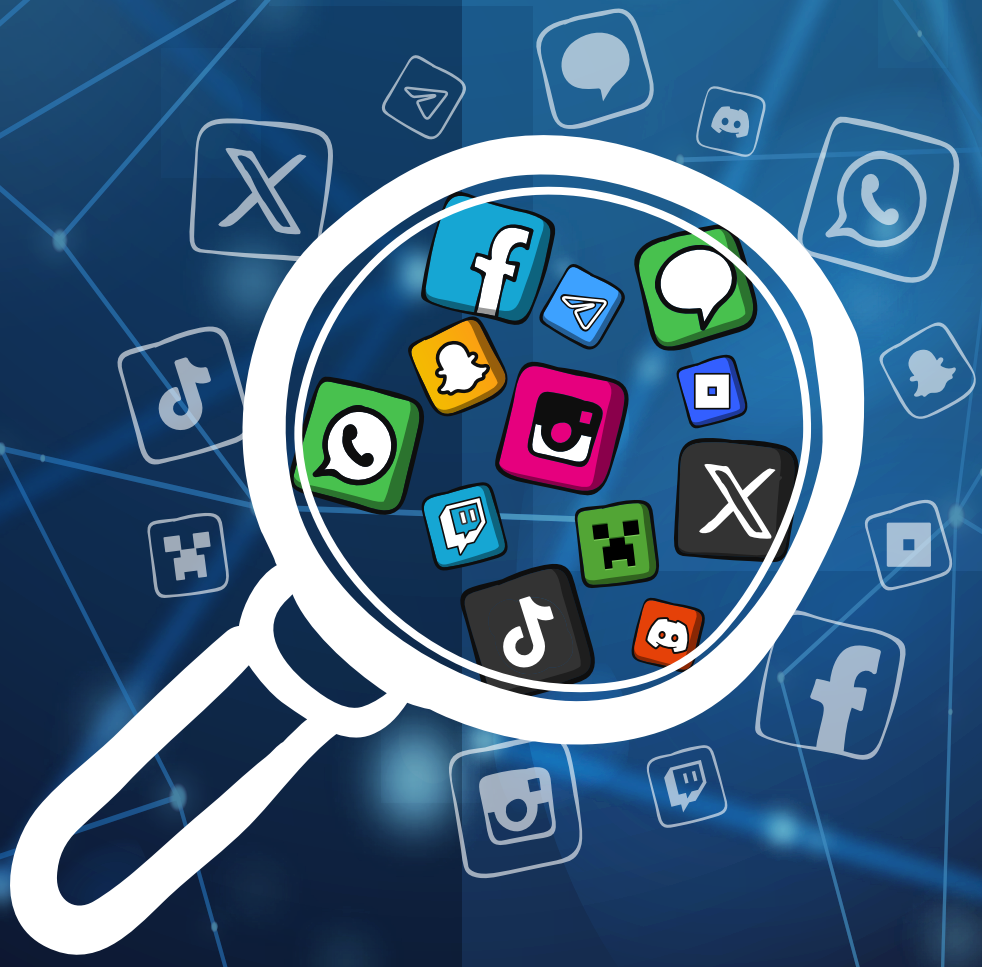
ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

RIESGOS Y PREVENCIÓN

Pérdida de privacidad en redes sociales



ANCI
AGENCIA NACIONAL
DE CIBERSEGURIDAD

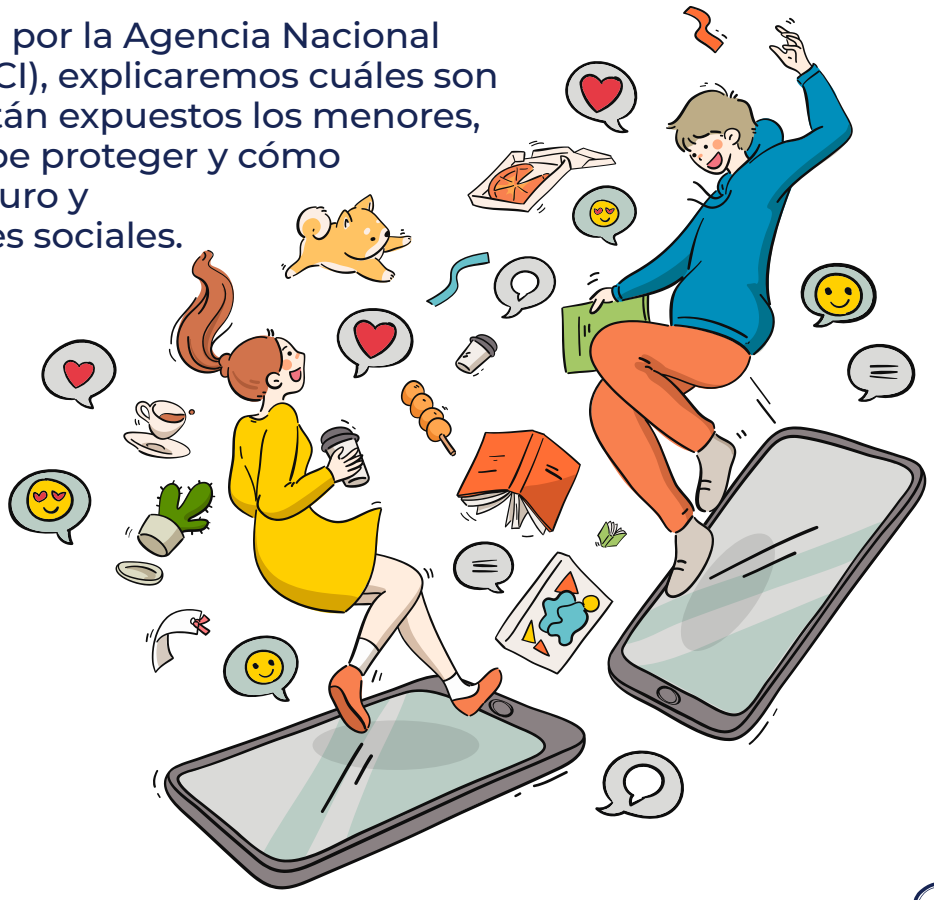
RIESGOS Y PREVENCIÓN

Pérdida de privacidad en redes sociales

La privacidad de los niños, niñas y adolescentes en Chile y en todo el mundo está siendo cada vez más expuesta, debido al tipo y a la cantidad de información que se publica en Internet.

Hoy, que suban una foto de ellos mismos, que compartan su ubicación en redes sociales o entreguen información personal en un juego online, entre muchos otros ejemplos, son acciones que tienen importantes riesgos asociados.

En esta guía, elaborada por la Agencia Nacional de Ciberseguridad (ANCI), explicaremos cuáles son los riesgos a los que están expuestos los menores, qué información se debe proteger y cómo apoyarlos en el uso seguro y responsable de las redes sociales.



PÉRDIDA DE PRIVACIDAD

En las redes sociales podemos compartir todo tipo de contenido: fotografías, videos, ubicación, datos personales, intereses, horas de conexión, etc. Muchas veces hacemos estas cosas sin recordar que nuestras aplicaciones constantemente recopilan y guardan información de lo que hacemos, como los sitios web que visitamos, los usuarios y contraseñas que ingresamos y los lugares en que navegamos, entre otros.

Todo esto expone nuestra vida privada, permitiendo potencialmente que otros accedan a ella, lo que debemos evitar para resguardar nuestra intimidad y la de niños y niñas.

Conductas que ponen en riesgo la privacidad:

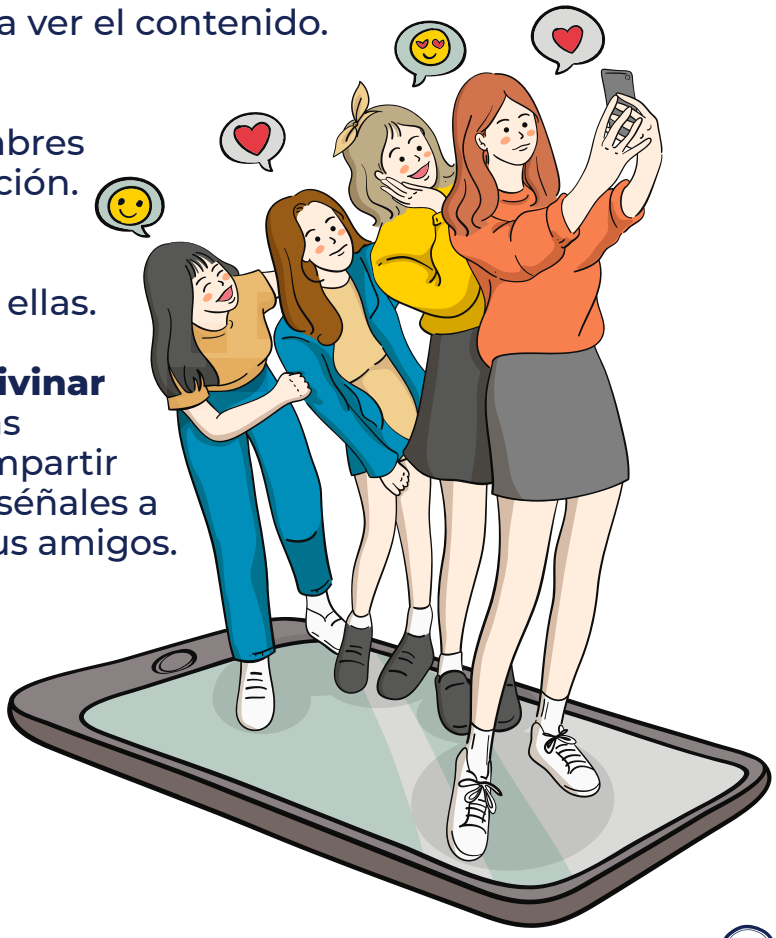
- **Tener un perfil abierto en redes sociales** para que cualquier persona pueda ver el contenido.

- **Publicar información personal** como el lugar de estudio, los nombres de sus familiares, teléfono y dirección.

- **Compartir fotos o videos** sin preguntar a quienes aparecen en ellas.

- **Usar contraseñas fáciles de adivinar por otros** o usar la misma en varias aplicaciones y sitios web. Evita compartir las claves con tus hijos e hijas y enséñales a que ellos tampoco lo hagan con sus amigos.

- **Aceptar a desconocidos** como amigos en redes sociales o en los juegos online.



RIESGOS Y PREVENCIÓN

Pérdida de privacidad en redes sociales

Subir contenido a Internet puede traer distintos riesgos que debes conocer:

• **Daños a la reputación:** Exponer contenido privado puede afectar negativamente la imagen de los niños, niñas y adolescentes.
Por ejemplo, subir una foto o video en que se muestre al menor en situaciones que consideremos graciosas puede ser motivo de burla por parte de sus pares hoy o en el futuro.

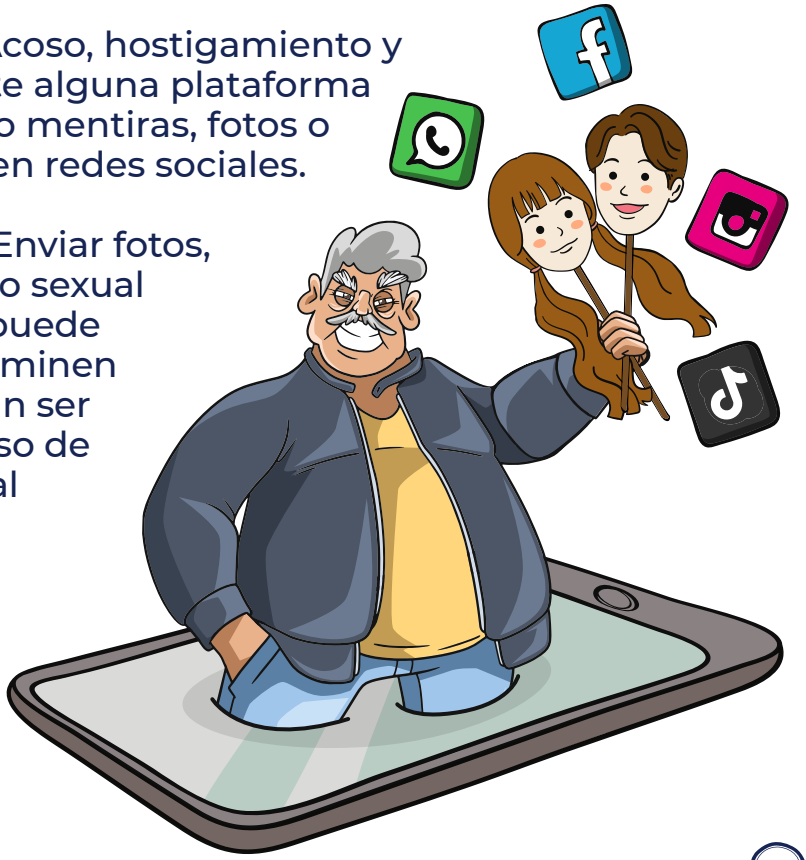
• **Suplantación de identidad:** Cuando las personas comparten información personal, facilitan la creación de perfiles falsos y pueden simplificar la deducción de contraseñas o preguntas de seguridad que permitan el acceso, por parte de terceros, a cuentas personales.

• **Riesgos para la seguridad personal:** Compartir nuestra ubicación, como domicilios, centros educativos o lugares habituales, así como también horarios o rutinas, permite que el menor pueda ser localizado físicamente por extraños.

• **Ciberbullying o ciberacoso:** Acoso, hostigamiento y humillación constante, mediante alguna plataforma o dispositivo digital, difundiendo mentiras, fotos o videos vergonzosos de alguien en redes sociales.

• **Sexting sin consentimiento:** Enviar fotos, mensajes o videos con contenido sexual explícito o sugerente a alguien puede permitir que estas imágenes terminen en manos equivocadas, o puedan ser usados para chantaje o, en el caso de menores de edad, como material pornográfico infantil.

• **Grooming:** Engaño por parte de un adulto hacia los menores para crear lazos emocionales y abusar de ellos sexualmente u obtener contenido pornográfico.



Recuerda que una vez que subimos algo a Internet, no se puede borrar.

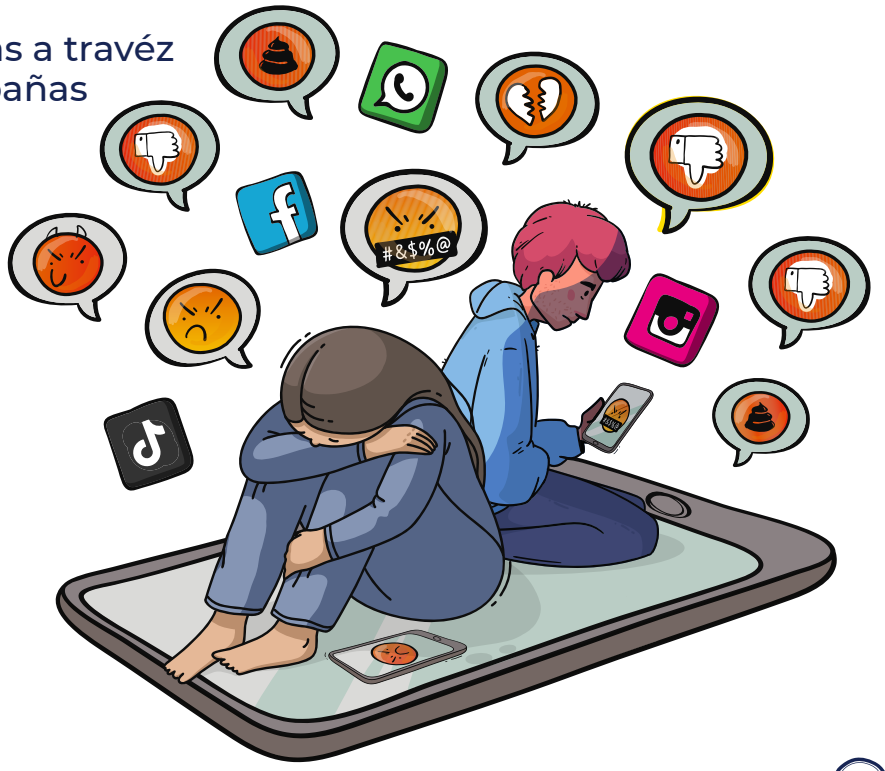
Otros riesgos a los que están expuestos los niños:

• **Contenido inapropiado:** Se refiere a publicaciones que muestran imágenes o videos violentos que promueven sentimientos de odio o que pueden poner en riesgo la salud de los menores.

• **Virus y malware:** Algunos sitios web o aplicaciones pueden contener programas maliciosos que son capaces de robar los datos personales, bloquear cuentas y dispositivos. Por ejemplo, si una persona descarga un malware puede perder acceso a la información de su teléfono o un tercero puede ingresar a su correo, suplantar su identidad e incluso transferir dinero desde sus cuentas bancarias.

• **Noticias falsas:** A través de sitios falsos se busca manipular a la opinión pública informando hechos que no son veraces.

• **Fraudes:** Estafas realizadas a travéz de Internet, como las campañas de phishing, mensajes maliciosos enviados por correo electrónico que buscan que la víctima ingrese a sitios web falsos para robar las contraseñas o los datos de las tarjetas bancarias.



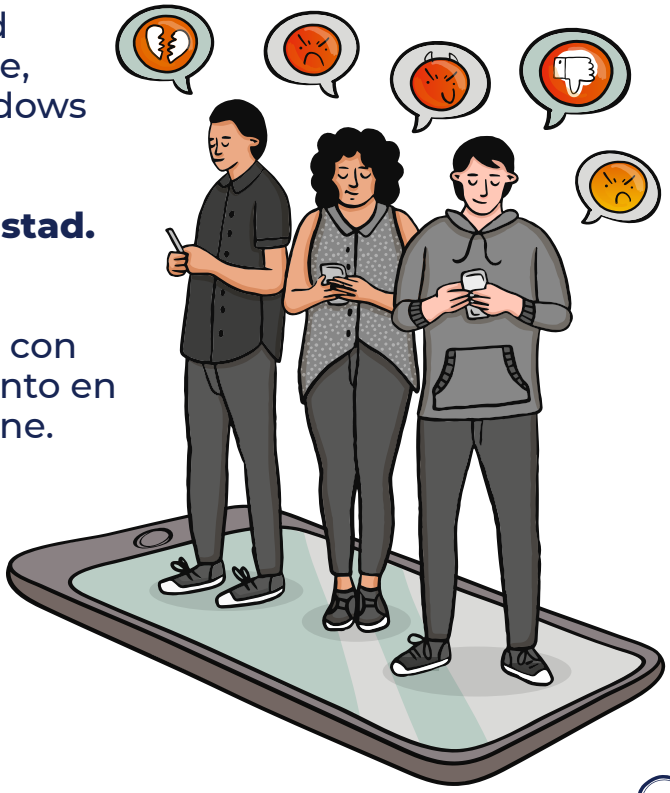
PREVENCIÓN

Existen diversas maneras de evitar los riesgos antes mencionados. La primera de ellas y la más importante es que los **adultos fomenten una comunicación sana y transparente con los menores**, manteniendo espacios de confianza, para que los menores sepan que pueden contarles a sus padres cualquier cosa que vivan en Internet sin miedo a castigos, y explicándoles los riesgos que existen al subir su información a Internet.

Otras medidas que es importante que integres a la dinámica digital de tu familia son:

- **Configura tus redes sociales en modo privado.**
De esta manera solo las personas realmente conocidas pueden ver lo que publicas.

- **Nunca compartas tus contraseñas.**
Se recomienda usar una distinta para cada aplicación y sitio web. Hay aplicaciones, como los gestores de contraseñas, que facilitan contar con una sola clave que proteja a todas las demás. Algunos de ellas son iCloud Keychain para los dispositivos de Apple, Credential Manager en Microsoft Windows y Bitwarden para Android.



- **Desconfía de quienes solicitan amistad.**
Hay personas que mienten sobre su identidad para obtener información, engañar, crear estafas o usar los datos con fines maliciosos. Esto puede ocurrir tanto en redes sociales como en los juegos online.

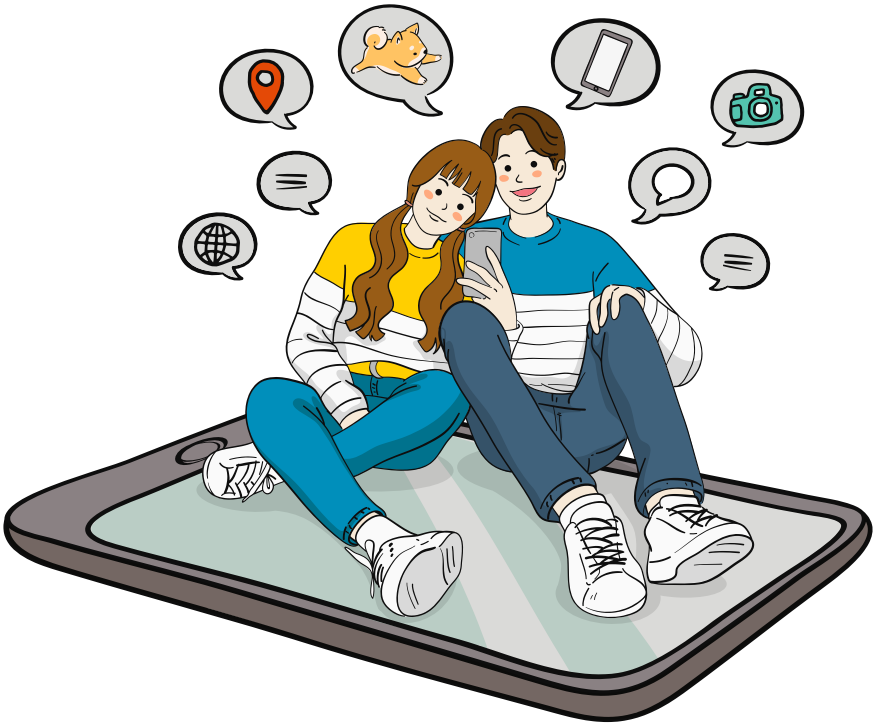
- **Siempre piensa antes de publicar.**
Al compartir contenido en redes sociales, reflexiona sobre las consecuencias que esto podría tener para ti y tu familia.

• **Crea claves largas y fáciles de recordar.**
Usa al menos cuatro palabras aleatorias, sin usar datos personales. Además, debes utilizar una diferente para cada sitio web, aplicación o juego online, y jamás las compartas con terceros.

• **Activa el bloqueo de pantalla**.
En lo posible, usa un segundo factor de autenticación (medida de seguridad que exige una forma adicional de identificación para acceder a una cuenta, la que se suma a la tradicional contraseña).

• **Cuidado con lo que publicas.**
Nunca se debe compartir en redes sociales o con desconocidos información personal como la dirección, RUT, nombre de familiares y mascotas, número de teléfono, estado civil, lugar de estudio o ubicación actual.

Dar el ejemplo en esto es clave, por lo que te recomendamos siempre tener en cuenta los riesgos asociados al uso de Internet.



ROL DE LOS PADRES O CUIDADORES

Los **adultos también tienen un rol clave en el cuidado de la imagen y privacidad de los niños, niñas y adolescentes**. Muchas veces los padres publican en sus redes sociales fotografías de los menores, una práctica que si bien parece inofensiva puede conducir a los riesgos antes mencionados.

Por este motivo, evita:

- Publicar imágenes o videos con uniforme escolar.
- Subir fotos de niños y niñas con poca ropa.
- Publicar información personal de tus hijos como el nombre, fecha de nacimiento u otros datos.

RECOMENDACIONES:

• **Supervisa** lo que hacen los niños, niñas y adolescentes en Internet, conoce sus gustos y amigos en línea.

• **Acompaña** a tus hijos(as) en Internet e incentívalos a compartir contigo sus actividades en línea.

• **Orienta** a los menores para tener una relación de confianza y así reforzar sus habilidades sociales.

• **Establece límites claros** en base a acuerdos con los menores. Ten una comunicación fluida con ellos, para que puedan definir juntos cuánto tiempo y dónde podrán estar en línea. Recuerda que es importante que accedan a contenido y plataformas acordes a su edad.

• **Utiliza control parental** para que sólo puedan acceder a contenido apropiado, limitando el tiempo y uso de la red. El control parental es una herramienta que existe en celulares o aplicaciones que permiten administrar, filtrar o restringir el acceso que menores de edad puedan tener en internet.

• **Enséñale a configurar sus redes sociales de forma segura,** manteniendo su perfil en modo privado, que sus fotos estén disponibles solo para los contactos y que no acepten a desconocidos.

¿QUÉ HACER SI MI HIJO(A) ES VÍCTIMA DE CIBERBULLYING O GROOMING?

Lo primero que debes hacer es apoyar al menor y nunca culparlo de la situación. Transmítele confianza y disponibilidad para ayudarlo(a).

En ambos casos, es importante denunciar a las policías o fiscalía para proteger a las víctimas y prevenir nuevos casos.

Ciberbullying:
- Para pedir orientación o denunciar, escribe al WhatsApp Violencia Digital de la PDI **+569 3459 9762**

Grooming:
Los canales de denuncia son:
- Teléfono PDI: **134**
- Programa **"Denuncia Seguro"**, Subsecretaría Prevención del Delito: ***4242** por teléfono fijo o celulares. El sitio web *www.denunciaseguro.cl* también está disponible.

Además, se recomienda:

- Bloquear a la persona en redes sociales y/o juegos o denunciar el perfil en la red social.
- No responder los mensajes.
- Guardar la evidencia, especialmente cuando hay un adulto desconocido involucrado.

Más información en:

www.denunciaseguro.cl
www.fiscaliadechile.cl
www.pdichile.cl

USO DE LA TECNOLOGÍA

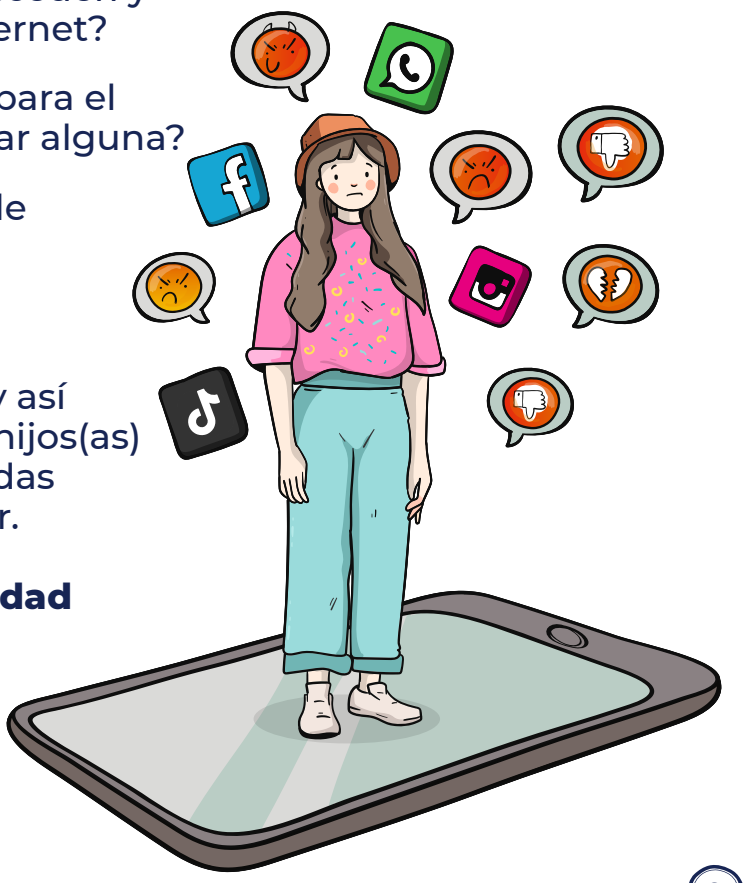
Queremos invitarte a reflexionar sobre el comportamiento, tanto tuyo como el de tus hijos(as), sobre el uso la tecnología. Lo importante es evaluar nuestras acciones y considerar la privacidad y seguridad como un tema relevante en nuestra sociedad.

Para ello, te proponemos responder las siguientes preguntas:

- ¿Sabes qué hace tu hijo(a) cuando está conectado a Internet?
- ¿Tu hijo(a) tiene cuenta en redes sociales?
- Si tiene redes sociales, ¿sabes a quiénes acepta como seguidores o a quiénes sigue?
- ¿Tu hijo(a) conversa con desconocidos?
- ¿Supervisas el contenido al que acceden y tiempo que tus hijos pasan en Internet?
- ¿Sabes que existen herramientas para el control parental? ¿Podrías nombrar alguna?
- ¿Usas como contraseña tu fecha de nacimiento, dirección, nombre de mascota u otro dato personal?

En base a lo explicado en esta guía puedes plantearte más preguntas y así analizar qué tan seguros están tus hijos(as) navegando en Internet y qué medidas puedes adoptar para guiarlos mejor.

Para más consejos de ciberseguridad ingresa a *anci.gob.cl*



RIESGOS Y PREVENCIÓN

Pérdida de privacidad en redes sociales

ANCI
AGENCIA NACIONAL DE CIBERSEGURIDAD