



GUÍA PARA PADRES Y ADULTOS RESPONSABLES

PROTECCIÓN DE LOS DATOS PERSONALES
DE NIÑOS, NIÑAS Y ADOLESCENTES EN LA WEB





con
vos
en la
web

www.convosenlaweb.gob.ar



INTRODUCCIÓN

Desde el Programa Nacional “Con Vos en la Web”, dependiente de la Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos de la Nación (en adelante, la PDP), consideramos necesario y útil que madres, padres y adultos responsables posean herramientas para el correcto uso de los datos personales de l@s niñ@s y adolescentes en Internet, especialmente en las redes sociales. Esta guía práctica presenta a los adultos, de manera simple y accesible, consejos y recomendaciones para proteger su privacidad.



Derecho a la privacidad y la protección de datos personales

La protección de los datos personales surge del derecho a la privacidad, que es uno de los derechos reconocido y garantizado en tratados internacionales de derechos humanos y en nuestra Constitución Nacional.

La privacidad incluye la forma en que las personas se ven así mismas y cómo deciden presentarse a los demás, es una condición indispensable para el libre desarrollo de la personalidad. Como parte del derecho a la privacidad se encuentran el derecho al honor, la intimidad y la imagen. En el caso de los niños, niñas y adolescentes, la Convención Internacional de los Derechos del Niño establece que no pueden ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

La Ley 25.326 de Protección de Datos Personales es una de las normas que protege el derecho a la privacidad. Su objetivo es garantizar el derecho que tienen todas las personas de conocer quién tiene sus datos, para qué los tiene y así tener control sobre ellos. La protección de datos que garantiza la ley incluye a los que circulan en internet.

¿Qué son los datos personales?

Toda la información que se relacione con una persona y que la identifique, o que pueda ser usada para identificarla.

Son datos personales: el nombre y apellido, el número de documento, la nacionalidad, el género, el estado civil, el número de teléfono, las huellas digitales y también la dirección de correo electrónico, el número de tarjeta de crédito o débito, el número de cuenta bancaria, las fotos, los videos, las publicaciones, entre otros.

Existe un grupo de datos personales, denominados datos sensibles, que exige mayor protección. Estos se refieren a ciertas circunstancias que hacen a la vida íntima de las personas y deben ser tratados de manera diferente, ya que requieren un mayor cuidado.

Son datos sensibles los que revelan: el origen étnico, las opiniones políticas, convicciones religiosas, filosóficas o morales, la afiliación sindical y la información referente a la salud o a la vida sexual.

Los datos personales en internet

Al navegar por la web encontramos datos personales, cuyo origen se puede dividir en:

- Los datos personales que se entregan de forma voluntaria, en las redes sociales, webs de compras en línea, etcétera.
- Los datos de navegación y de comportamiento en la red.
- Los datos personales publicados por terceros, es decir, no proporcionados por los titulares.

Los Datos Personales y la Reputación web de los niñ@s y adolescentes

Es importante tener en cuenta que la vida digital de los niñ@s nace con que ellos, cuando los padres y familiares comienzan a publicar sus fotos de bebé o contenidos relacionados con ellos en las redes sociales. En algunos casos, incluso antes de nacer los niñ@s tienen vida digital, por ejemplo: cuando se comparten ecografías por redes sociales.

Internet es una gran herramienta, pero es importante que se la utilice con responsabilidad.

Muchas veces se encuentran en internet contenidos sobre los niñ@s que las madres, padres, familiares o adultos cercanos publican. Una vez en la web, estos contenidos que son datos personales de los niñ@s y adolescentes, se replican, comienzan a aparecer en los buscadores y pueden alcanzar gran difusión.

Esto ocurre cuando los padres publican en su red social imágenes de sus propios hijos, o imágenes de sus hijos con compañeros de colegio, o cuando familiares publican imágenes en el marco de encuentros familiares, etc.

Internet es un espacio público y, como tal, no se puede controlar ni tener conocimiento de todas las personas que ingresan en los distintos sitios y acceden a determinada información personal.

Qué consecuencias puede tener descuidar los datos personales de los niñ@s y adolescentes en la web

Que sean usados por personas que no están autorizadas y que, en algunas casos, no tengan buenas intenciones.

Que puedan facilitar situaciones de Grooming (acoso sexual por parte de un adulto a través de internet) o cyberbullying (hostigamiento, discriminación, amenazas, acoso por parte de otro/s niñ@s o adolescente/s a través de internet).

Que dañen su reputación web, ya que habrá información relacionada para siempre con ellos sobre la que no tuvieron posibilidad de decidir.

La Reputación web

Es la imagen y el prestigio que las personas tienen en internet. Se genera a raíz de toda la información online referida a ellas y se construye por acción propia, de terceros e incluso por omisión.

• **Acción propia:** consiste en las publicaciones que hacen las personas en las redes sociales, blogs, sitios web, grupos o foros aclarando su identidad.

• **Acciones de terceros:** son las publicaciones en donde se cita o nombra a otras personas (etiquetas, menciones, respuestas, etc)

• **Omisión:** no tener cuentas en redes sociales o participación web, es de por sí un dato que forma parte de la reputación y es tomado en cuenta cuando se busca información sobre una persona.

El rol de los adultos en el cuidado de la reputación Web de niñ@s y adolescentes

En el caso de los niñ@s y adolescentes, el comportamiento de los padres y adultos responsables en internet es muy importante para la constitución de su reputación web. Lo primero a tener en cuenta, es que toda información que se sube a la web, relacionada con niñ@s y adolescentes quedará (probablemente) para siempre asociada a su nombre.

La reputación web se construye a lo largo de años y es difícil de modificar ya que en Internet no hay olvido. Si bien, se puede pensar que al borrar una publicación esta se elimina; es importante tener presente que otra persona puede haber descargado, compartido o guardado el posteo o el contenido y por ende volver a subirlo y compartirlo.

Estas son algunas de las situaciones donde la reputación web se vuelve importante:

Búsqueda laboral: debido a la penetración de Internet, futuros jefes o entrevistadores buscan referencias en la web. Para hacerlo, ponen el nombre del postulante al puesto en los buscadores y analizan todas las referencias que aparezcan.

Muchas veces, en las redes sociales de niñ@s y adolescentes aparecen contenidos relacionados con ellos pero subidos por sus madres, padres u otros adultos cercanos, que develan aspectos de su vida privada. Estos contenidos, vistos por un posible futuro jefe, podrían ser considerados negativamente.

Cita: una práctica cada vez más común, sobre todo entre los jóvenes, es buscar en la web a las personas antes de un primer encuentro.

Podría suceder que en el futuro, los niñ@s y adolescentes se avergüencen o se vean perjudicados por los contenidos relacionados con ellos, que hoy suben los adultos a internet.

Intercambio Profesional: en el ámbito profesional es habitual que, previamente a realizar tareas comunes o intercambios, las personas se busquen en la web para conocer mejor sus trayectorias.

Podría ocurrir que las futuras relaciones profesionales de los niñ@s y adolescentes se vean afectadas por contenidos subidos por sus madres, padres o adultos cercanos.



Recomendaciones antes de publicar o compartir imágenes y /o contenidos sobre niñ@s y adolescentes a las redes sociales

- **Como consejo general, siempre pensar antes de publicar.** Al igual que la seguridad física, la seguridad digital de l@s niñ@s y adolescentes comienza con los padres y adultos responsables, en especial cuando son pequeñ@s. En el mundo digital puede haber personas que recolecten información sobre menores de edad con fines desconocidos.

- No publicar, compartir o etiquetar información personal sobre niñ@s y adolescentes sin su autorización, ellos tienen derecho a cuidar su imagen.

Aunque sean bebés o niñ@s pequeñ@s, es importante recordar que en internet la información es muy difícil de borrar, y en el futuro ellos podrían preferir que esos datos no estén en la web.

- Si se decide subir información sobre niñ@s y adolescentes:

1 Seleccionar quiénes pueden acceder a la información que publicamos sobre niñ@s y adolescentes.

Configurar la privacidad en las redes sociales utilizadas, de esta forma, se puede tener más control sobre quiénes podrán ver las fotos y publicaciones.

En Facebook, también se pueden armar listas entre los contactos para seleccionar quién verá cada publicación. Por ejemplo: "Familia", "Compañeros de trabajo", etc. De esta forma, al subir un contenido se puede elegir que lo vea determinada lista.

En Twitter se puede proteger la privacidad de los tweets. De este modo solo los seguidores y usuarios que se aprueben, podrán verlos.

2 Evitar que en las fotos y videos publicados se reconozca el colegio, club u otra institución a la que el niño, niña o adolescente pertenece. Para esto es importante:

No publicar imágenes de la puerta o de algún espacio característico de esos establecimientos.

No compartir actividades, fotos o promociones de la institución educativa o club.

No subir fotos en las que l@s niñ@s o adolescentes aparezcan con uniformes, escudos o logos.

Quitar la opción de geolocalización del celular o Tablet.

3 -No publicar datos que expongan a l@s niñ@s y adolescentes a situaciones de riesgo.

No publicar imágenes donde aparezca la dirección de la casa o patente del auto familiar.

No hacer publicaciones que indiquen que el niño o niña estará sin acompañamiento adulto. Por ejemplo: viajes que hará con amig@s, actividades a las que vaya a concurrir o momentos donde vaya a quedar sol@ en su casa.

No compartir fotos de compañer@s de guardería, jardín o colegio sin el consentimiento de sus padres.

Quitar la opción de geolocalización del celular al momento de sacar una foto que será compartida en las redes sociales.

4 Utilizar contraseñas seguras.

No usar la misma clave para todo. Tener una contraseña distinta para cada cuenta (mail, Facebook, Tweeter, etc.) y dispositivo (PC, Tablet, celular). Usar claves extensas y complejas; fáciles de recordar, pero difíciles de olvidar y de adivinar. Las mejores contraseñas (difíciles de adivinar y por ende de ser sustraídas) son las largas, que contienen letras, números, signos de puntuación y símbolos. Hay palabras o frases inventadas por el usuario que pueden ser fáciles de recordar para él mismo e imposibles de descifrar para quien lo intente. Para muchos, las contraseñas complejas son un riesgo por la posibilidad de olvidarlas. Un truco es usar una palabra o frase fácil, pero cambiando las vocales por números.

Por ejemplo:

'Tengogoparadecirte'
sería
"T3ng0alg0parad3c1rt3".

No compartirlas con nadie.

Las claves son personales y no deben ser compartidas con nadie. El usuario es el dueño de la cuenta, pero también es el dueño de la clave. La

misma no debe ser conocida más que por su dueño.

Evitar información personal, ya que es fácil de adivinar

No incluir nombre, apellido, fecha de nacimiento, número de documento o información del estilo.

Procurar cambiar la clave luego de un período de tiempo prudencial.

Elegir preguntas secretas o de seguridad que sean complicadas de adivinar.

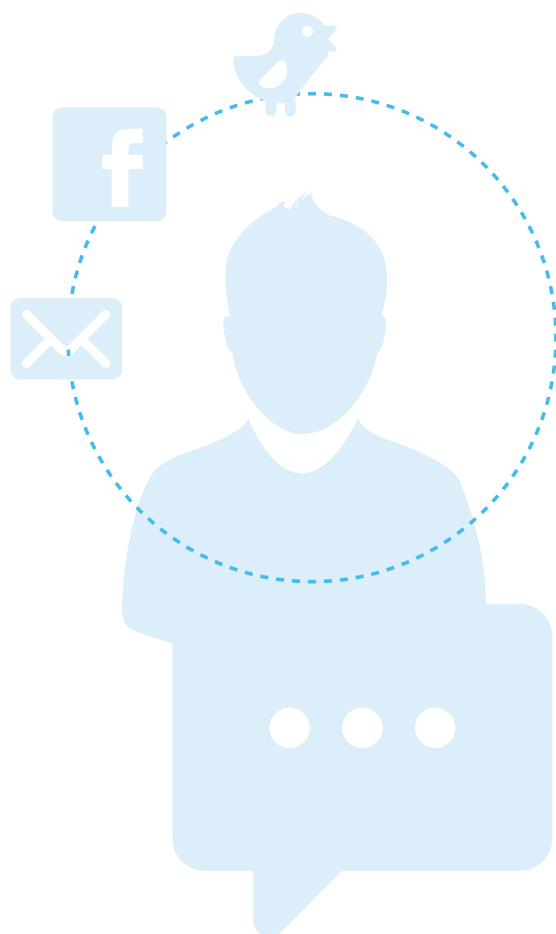
Al crear cuentas de usuarios debemos seleccionar una "Pregunta Secreta" o de "Seguridad" para usar en caso de olvidar la clave o contraseña de acceso. Es recomendable elegir las que sean más complicadas de adivinar, evitando las de respuestas obvias. Ejemplo: Color favorito.

Guardar las claves en un documento de texto.

Al elegir contraseñas largas, difíciles de memorizar, y tener varias (para los distintos usuarios con los que contamos) puede ser útil tenerlas almacenadas en un documento dentro de nuestra PC. Esto puede ser pesado o tedioso, pero es muy seguro.

- Compartir con los familiares y amig@s los consejos anteriores.





ASESORAMIENTO Y CONSULTAS
Escribinos a convosenlaweb@jus.gob.ar





con vos en la web

Un programa de la



PDP

Dirección Nacional de
**Protección de
Datos Personales**

Protegé tu **PRIVACIDAD**,
resguardá tus **DATOS PERSONALES**.

Buscanos en:

www.jus.gob.ar/datospersonales

Contactanos:

convosenlaweb@jus.gob.ar



Seguinosen: @convosenlaweb



Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación