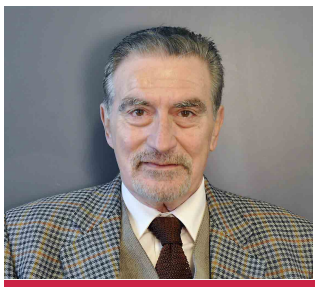
AGOSTO2016

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires

GUÍA BÁSICA DE DERECHOS
PROTECCIÓN DE DATOS PERSONALES EN INTERNET

Atención al Vecino Av. Belgrano 673
0800 999 3722

defensoriacaba
www.defensoria.org.ar



EDUARDO PEDUTO
Titular del Centro de Protección
de Datos Personales

GUÍA BÁSICA DE DERECHOS PROTECCIÓN DE DATOS PERSONALES EN INTERNET

Actualmente es común escuchar que vivimos en la “sociedad de la información”. Esta es la manera en que se ha denominado a la sociedad del siglo XXI que ya no está caracterizada por el desarrollo industrial sino que se centra en el flujo de la información.

En este contexto, con la llegada de Internet y de las Tecnologías de la Información y Comunicación (TIC) el acceso a la información es más sencillo, rápido y tiene un alcance que borra las fronteras actuales del mapa mundial.

Internet, como parte de estas tecnologías, es una herramienta sumamente útil para cada una de las actividades que realizamos a diario, como trabajar, estudiar, comunicarnos, entretenernos, entre otras. Por tal motivo, es importante aprender a dominarla.

Tanto para los denominados “nativos digitales” -que son las personas que han nacido y crecido con las TIC y poseen un gran dominio de ellas-, como para los “inmigrantes digitales”, -quienes no han nacido ni crecido con este tipo de tecnología, pero la han adoptado-, es clave entender los derechos, obligaciones y también los riesgos que podemos encontrar en el ecosistema de Internet.

Por la forma en que circula la información en la Red, uno de los derechos que adquiere especial relevancia es el de la protección de datos personales y la privacidad.

Cuando protegemos datos protegemos personas. Esta es la esencia de nuestra acción como Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad Autónoma de Buenos Aires. Esta convicción y este compromiso lo desplegamos en todos y cada uno de los campos en los que intervenimos: en la divulgación y promoción de derechos, en la capacitación, en la investigación y cuando receptamos denuncias sobre la vulneración de datos personales. Por ello, hacemos hincapié en que cuando nos abocamos a la protección de datos personales estamos protegiendo personas. ¿De qué manera? Protegiendo su intimidad, su privacidad, su dignidad en el marco del ejercicio de su ciudadanía, entendida esta en el sentido amplio en que hoy es reconocida por el desarrollo de las ciencias sociales. En definitiva, estamos protegiendo su mayor atributo que es su condición de ser humano.

Todas estas cuestiones adquieren especial relevancia cuando los actores que están en juego o pueden verse involucrados son niños, niñas y adolescentes. Por tal motivo es que estamos trabajando activamente en escuelas, en organizaciones sociales, en instituciones juveniles, para que las nuevas tecnologías de información y comunicación sean herramientas útiles en el desarrollo de todas las personas y no un reducto privilegiado para iniciados o especialistas.

Esta guía es también parte de este trabajo, los invitamos a reflexionar sobre el modo en que protegemos nuestra información personal al utilizar Internet.

¿QUÉ ES INTERNET?

Internet puede definirse como un conjunto descentralizado de redes de comunicación interconectadas. Los dispositivos que se conectan a Internet pueden comunicarse entre sí gracias a la utilización de un lenguaje en común: el protocolo TCP/IP.
Esta definición puede parecer compleja, pero es importante que sepamos que Internet, tal y como la conocemos hoy en día, se basa en la idea técnica de una arquitectura abierta –que permite añadir, modernizar o cambiar sus componentes– donde no existe un solo punto que centralice la información.

¿CUÁNDO NACE INTERNET?

Durante sus primeros años, Internet se desarrolló gracias a los esfuerzos entrelazados, pero independientes, de muchas personas de la academia y del gobierno de Estados Unidos.
En 1969, ARPANET, una red de investigación formada por cuatro universidades conectadas entre sí, realizó su primera conexión y se convirtió en la base de Internet. En términos técnicos, hay tres hitos en la evolución de la tecnología que permitieron llegar a Internet tal como lo conocemos hoy:
1. Década del 60: la invención de la conmutación de paquetes que facilita el envío de paquetes de datos.
2. Década del 80: el desarrollo del protocolo TCP/IP que permite que los dispositivos hablen el mismo idioma.
3. Década del 90: se inventó el HTML (lenguaje estándar para crear sitios web) y el HTTP (que permite la comunicación de los navegadores y servidores web), que sentaron las bases para la World Wide Web (www).

¿QUÉ SON LAS REDES SOCIALES?

Internet funciona como medio de transmisión de servicios y aplicaciones, tales como la World Wide Web (www), el correo electrónico, las redes sociales, el streaming, la mensajería instantánea o los juegos en línea, entre muchos otros.
De este modo, las redes sociales son plataformas que funcionan a través de Internet y nos permiten relacionarnos con otras personas y compartir información. Hay distintas redes sociales, cada una con una lógica propia. Las más usadas son Facebook, Twitter e Instagram.

¿QUÉ PASA CON EL RESPETO DE LOS DERECHOS HUMANOS EN INTERNET?

En el contexto actual la mayoría de los procesos de la vida cotidiana están mediados por Internet. Las actividades comerciales, el ocio y entretenimiento, la investigación y el estudio adquieren otras dimensiones a partir del uso masivo de esta red de redes. Si bien esto trae aparejado beneficios sociales, económicos y ofrece oportunidades sin precedentes para el desarrollo de los derechos humanos, también arrastra consigo violaciones a estos derechos.
Es por esto que debemos recordar que los derechos humanos son inherentes a toda persona, universales, inalienables e indivisibles, y como tales deben ser garantizados siempre. Esto significa que tampoco puede haber una división entre el plano online –lo digital– y offline –lo analógico– cuando se trata de los derechos de las personas.
Internet debe ser un espacio que garantice y que ofrezca oportunidades para el desarrollo de los derechos humanos.

¿QUÉ SON LOS DATOS PERSONALES?

Hoy en día, por el constante crecimiento de la Red, podemos afirmar que cada vez más personas publican información online. Sin embargo, muchas veces esta acción no se percibe como tal porque no existe un conocimiento claro sobre lo que es un dato personal.
Los datos personales son información de cualquier tipo que hace identificable a una persona: el nombre, el apellido, el DNI, el número de tarjeta de crédito y el teléfono forman parte de esta categoría.
Si bien son los primeros que se nos vienen a la cabeza, estos no son los únicos dado que hay más información que hace posible la identificación. Agregamos entonces que los gustos, intereses y las opiniones también son datos personales.
Asimismo, la información personal no se materializa sólo en textos, sino también en vídeos, imágenes e inclusive la voz.
Todos estos datos son muy importantes porque revelan una gran cantidad de información sobre una persona: la identidad, la forma de contactarla, el lugar de procedencia u origen, aficiones, preferencias, hábitos de consumo, etc.

¿QUÉ SON LOS DATOS SENSIBLES?

Dentro de los datos personales se encuentra un tipo de datos que requiere mayor protección que los demás. Se los llama “datos sensibles” y son los que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir algún trato discriminatorio.

¿POR QUÉ ES IMPORTANTE LA PROTECCIÓN DE DATOS PERSONALES EN INTERNET?

La protección de datos personales y la privacidad son derechos garantizados en nuestro país por diversas leyes, la Constitución Nacional y tratados de derechos humanos. Al ser un derecho humano, como se dijo antes, éste también debe ser respetado en Internet.

En sus comienzos, Internet se utilizaba, básicamente, para buscar información y para enviar y recibir correos electrónicos. No mucho después, el uso de blogs, el pago de cuentas online, la oportunidad de subir fotos y compartir información personal en redes sociales se volvió esencial para el desarrollo de la Red. Esta posibilidad de publicar y hacer circular contenido de todo tipo generó un verdadero cambio en las prácticas sociales y, por supuesto, en la protección de datos personales. En este contexto, se vuelve necesario contar con información y herramientas para proteger nuestro derecho.

¿CÓMO CIRCULAN NUESTROS DATOS EN INTERNET?

Podemos decir que nuestros datos personales circulan por Internet de tres formas:

1. Los datos entregados en forma voluntaria

Cuando somos nosotros mismos quienes los damos. Un claro ejemplo es todo lo relativo a las redes sociales: desde el momento en que abrimos una cuenta y, luego, subimos fotos, relatamos hechos, comentamos posteos, damos “me gusta”, etc.

2. Datos proporcionados por otras personas

En este caso es otra persona quien sube a Internet datos nuestros. Hay diversas formas en las que esta conducta se puede ver: la más simple es la publicación de posteos y de fotos en redes sociales. También es posible la publicación de datos por parte de algún organismo estatal o de empresas privadas.

3. Datos de navegación y comportamiento

Lo que hacemos en Internet deja rastro a través de los datos de navegación y comportamiento. La forma más utilizada para almacenar estos datos es a través de los programas conocidos como cookies. Éstas son herramientas que permiten el registro de nuestras conductas y comportamientos que pueden utilizarse tanto para mejorar la navegación del usuario (recordando contraseñas, por ejemplo) como para ofrecer publicidad en la Red basada en nuestros hábitos.

¿QUÉ ES IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE?

La Identidad digital es toda la información sobre una persona que se encuentra en Internet circulando por las tres maneras explicadas en el apartado anterior (entregados voluntariamente, otorgados por terceros o por el uso de las cookies). Sin embargo, hay otro concepto importante: el de reputación online. Este se focaliza en la opinión formada por otros acerca de una persona en base a la información que encuentran en Internet, es decir, en relación a la identidad digital.

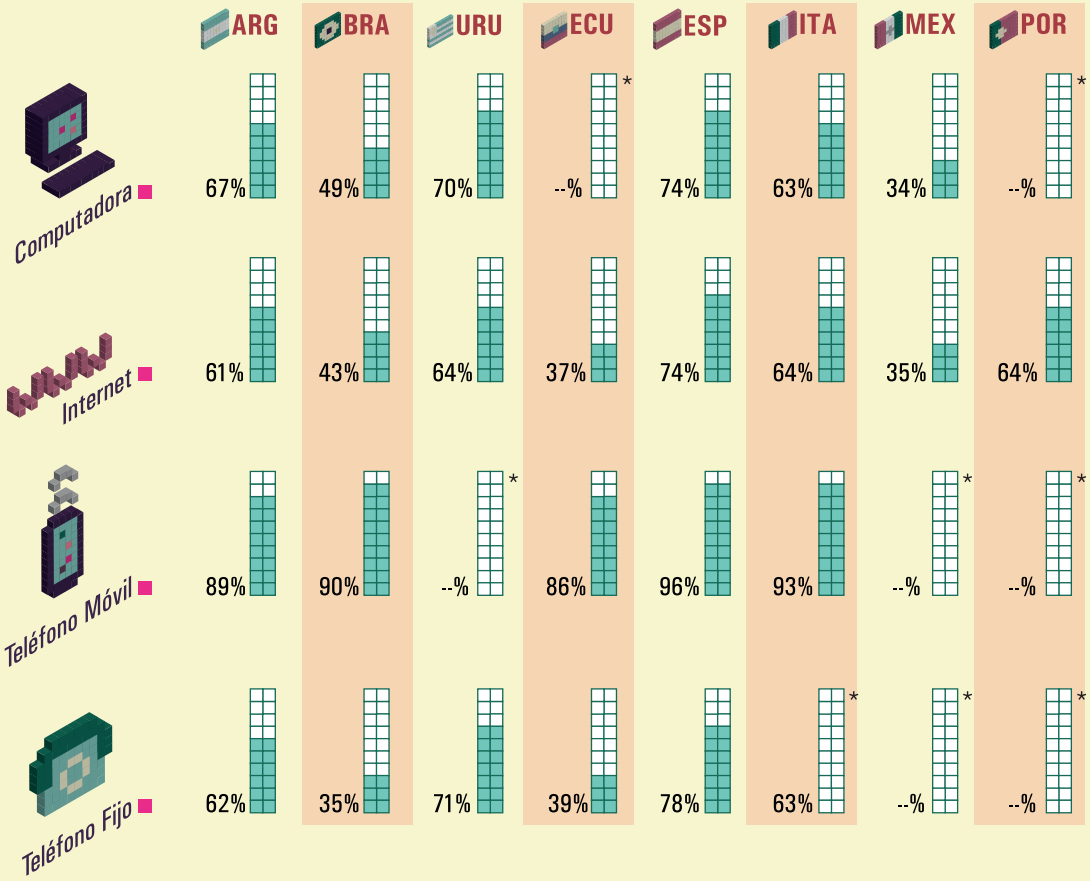
¿QUÉ ES EL *SEXTING*?

Sexting es un término inglés conformado por la unión de dos palabras: sex (contenido sexual) y texting (textear/enviar mensajes), y que refiere al envío de imágenes/videos de contenido sexual a otra/s persona/s tanto a través de distintos servicios de mensajería instantánea como de redes sociales, correo-e y foros.

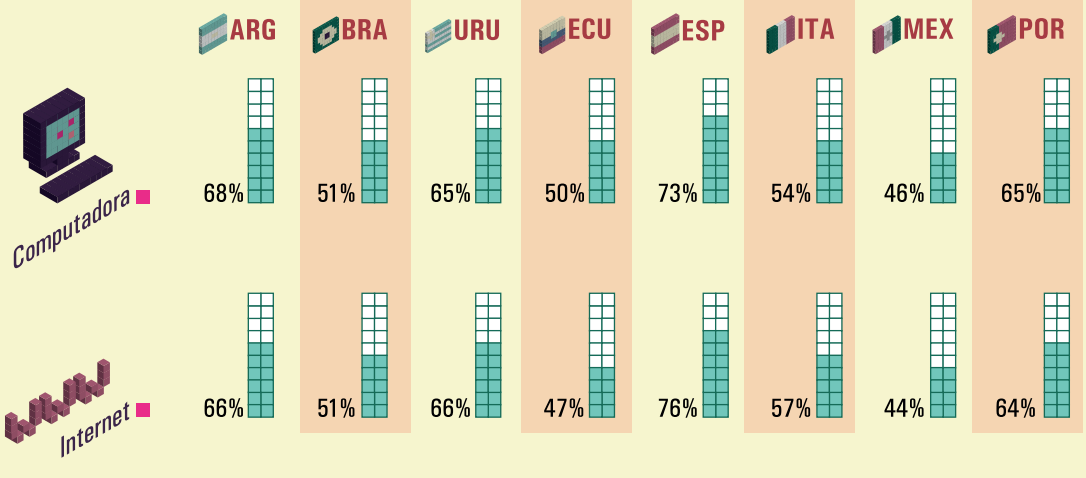
En general, lo que se difunde son imágenes personales y más específicamente, imágenes relacionadas con la sexualidad (a los que antes llamamos datos sensibles). Si bien el envío de fotos se hace entre dos personas o un grupo, la circulación de la imagen puede derivar en que la misma sea publicada en un sitio web o viralizada.

Si bien el sexting se lleva a cabo tanto por jóvenes como por adultos, es una práctica muy usada entre los adolescentes.

Porcentaje de hogares urbanos con acceso



Porcentaje de personas que utilizan



Fuente: INDEC * Sin datos

¿POR QUÉ DEBO CUIDAR MI INFORMACIÓN?

Todo lo que subimos a Internet queda en Internet. Esta es una idea que debemos aprehender y es uno de los motivos centrales por el cual cuidar nuestra información es central. Es muy complicado lograr la eliminación de información que se encuentra en la Red. La capacidad de duplicación del material que permite la informática, la velocidad con la que se hace sumado a la eliminación de fronteras que produjo Internet, generaron la imposibilidad de controlar la información en general y los datos personales en particular.

Por ello, es importante mantener un cierto control de aquellos datos personales que circulan en Internet. Ese control debe materializarse en acciones, como prestar atención a la información que nosotros mismos subimos y en tomar conciencia de que otras personas también pueden subir datos nuestros.

¿QUÉ RIESGOS Y AMENAZAS EXISTEN EN INTERNET?

Hay muchas y muy diversas formas de ataque a los datos personales. Las mismas van cambiando a lo largo del tiempo y van adquiriendo múltiples y nuevas modalidades a medida que se generan avances tecnológicos.

Si bien pueden ser muy distintas unas de otras, todas tienen la misma finalidad: acceder a información personal de los usuarios, ya sea para fines delictivos, fines de espionaje o fines comerciales. Las amenazas informáticas más conocidas son los distintos tipos de malware o software maliciosos (ver glosario) que tienen el objetivo de introducirse en cualquier dispositivo electrónico para alterar sus sistemas, robar datos y tomar control remoto de ellos.

En general, solemos ver los riegos relacionados con la tecnología como factores externos al uso que cada uno le da a Internet, y muchas veces no los percibimos como derivados de las propias prácticas.

Es por eso que creemos necesario nombrar tres prácticas actuales que tienen consecuencia en la protección de nuestros datos personales y en nuestra privacidad: el *sexting*, el *ciberbullying* y el *grooming* (Ver págs. 4, 8 y 9).

¿CÓMO PUEDO PROTEGER MIS DATOS PERSONALES EN INTERNET?

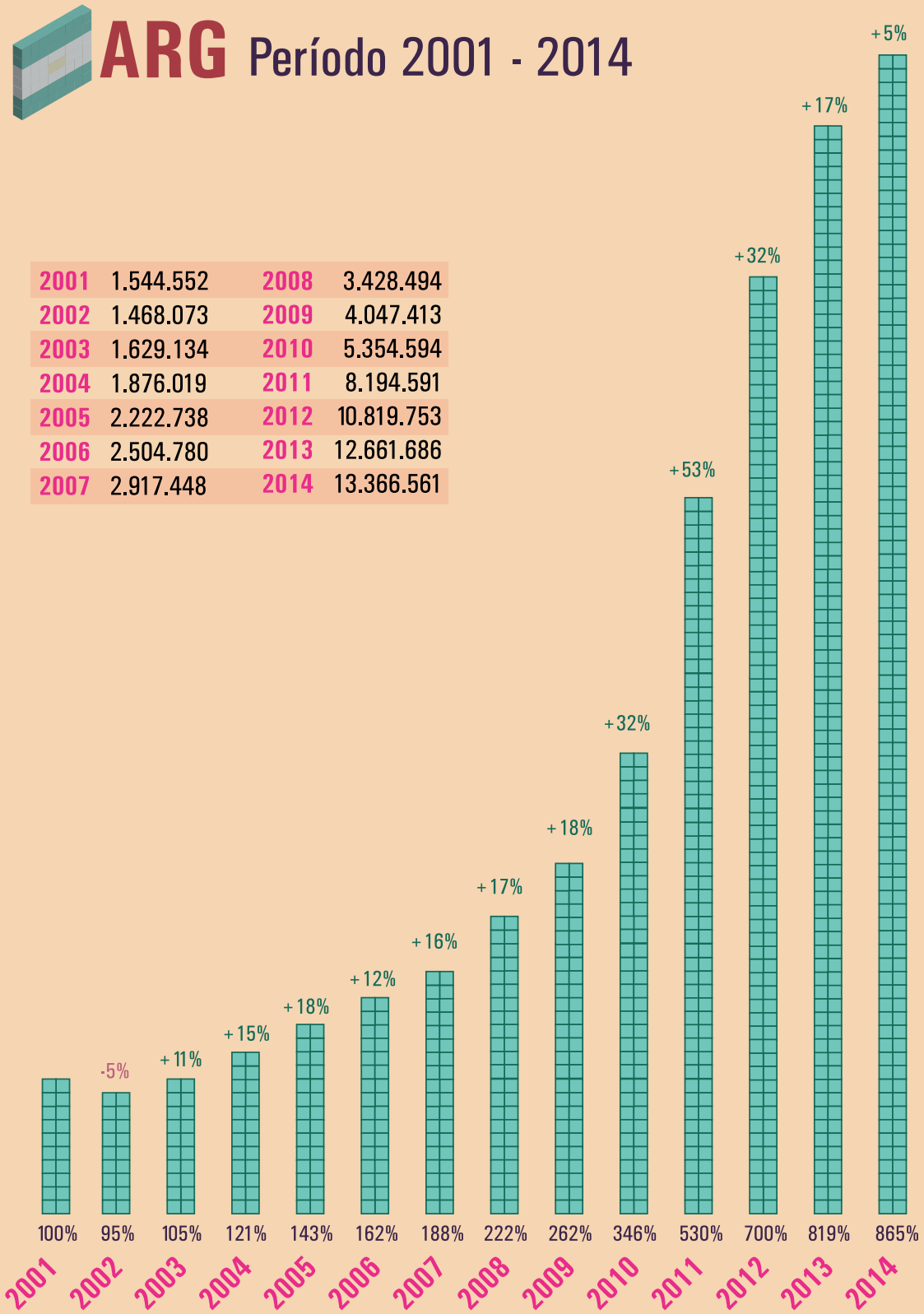
Es necesario remarcar que los datos y la información que circula en Internet son difíciles de borrar. Sin embargo, podemos proteger nuestros datos personales tomando en cuenta los siguientes consejos:

- Configuración de la privacidad en redes sociales: cada red social posee su propia configuración de privacidad. Con los ajustes adecuados podés elegir quiénes pueden ver lo que publicás, con quién compartís el contenido y, en algunos casos, ser notificado cuando te etiquetan en alguna publicación. Cuando abrimos una cuenta, todos nuestros datos se encuentran públicos por defecto y cada uno de nosotros debe saber que puede configurarlo.
- Contraseñas: La configuración de las contraseñas es el primer paso para resguardar nuestros datos personales. Para que sean efectivas, tienen que ser secretas. Las claves más seguras deben ser largas y combinar números, letras y caracteres.
- Uso de WiFi público: Los puntos de conexión WiFi públicos son cada vez más. Te aconsejamos que, al usar este tipo de redes, el envío de información personal se realice únicamente por medio de un sitio web codificado (https). Esto es importante ya que, al utilizar tales redes, desconocemos quién las administra o qué medidas de seguridad se utilizan para proteger la información que circula por ellas.
- Descarga de APP: Al descargar algunas aplicaciones te pueden solicitar autorización para acceder a tu dispositivo, conocer tus datos de contactos, ubicación y sincronizar tus cuentas en redes sociales, etc. Para evitar que tus datos se usen con otros propósitos, informate sobre la aplicación y prestá atención a los permisos que aceptás al descargarla.

Internet Cantidad de accesos residenciales, crecimiento interanual y total.

ARG Período 2001 - 2014

2001	1.544.552	2008	3.428.494
2002	1.468.073	2009	4.047.413
2003	1.629.134	2010	5.354.594
2004	1.876.019	2011	8.194.591
2005	2.222.738	2012	10.819.753
2006	2.504.780	2013	12.661.686
2007	2.917.448	2014	13.366.561



Fuente: SINCA

¿QUÉ ES EL *CIBERBULLYING*?

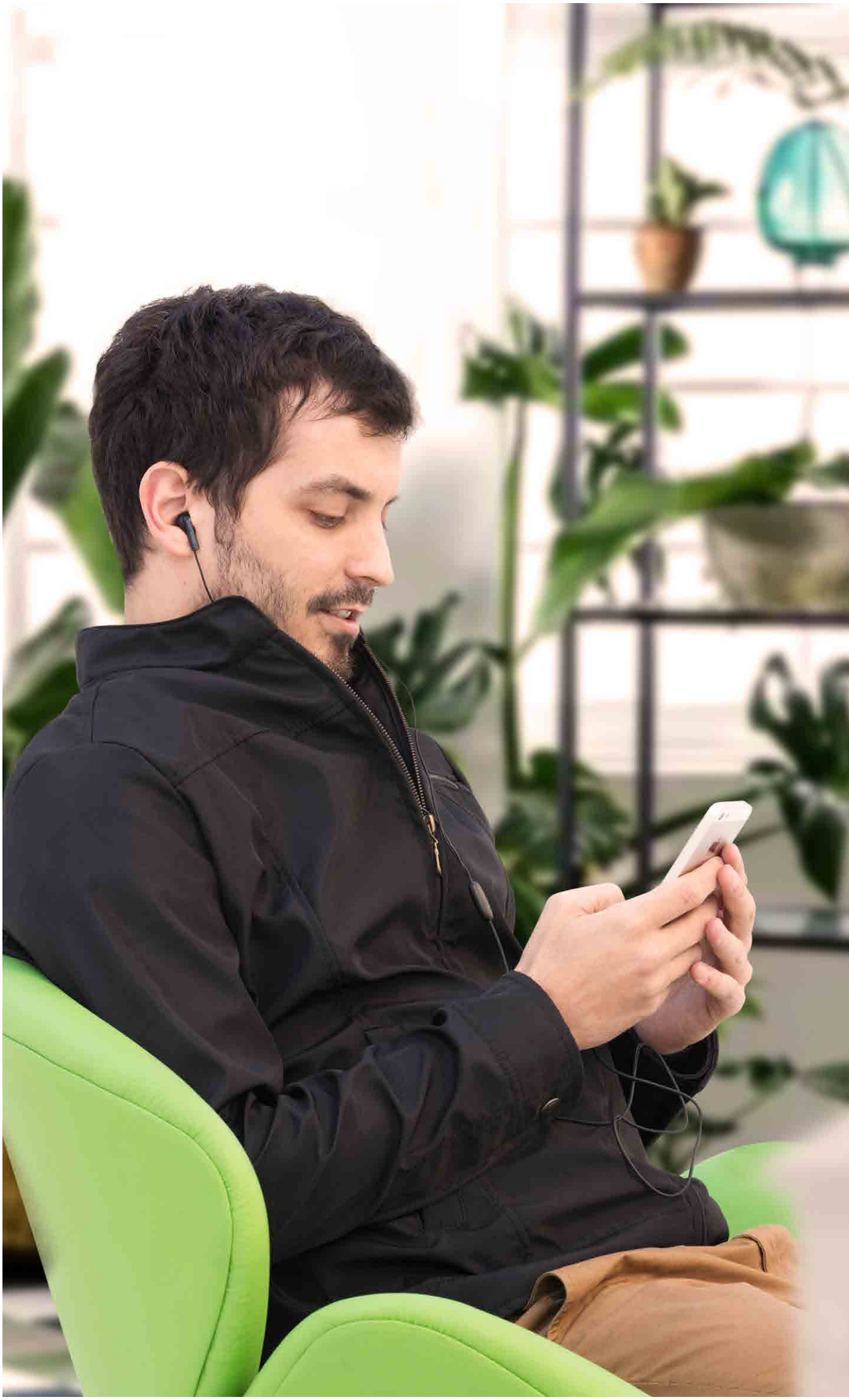
El ciberbullying es llevar la ya conocida práctica del bullying –u hostigamiento escolar– al plano online. Consiste en el uso y difusión de datos difamatorios y discriminatorios a través de las diferentes plataformas y herramientas que ofrece Internet, como las redes sociales y la mensajería instantánea.

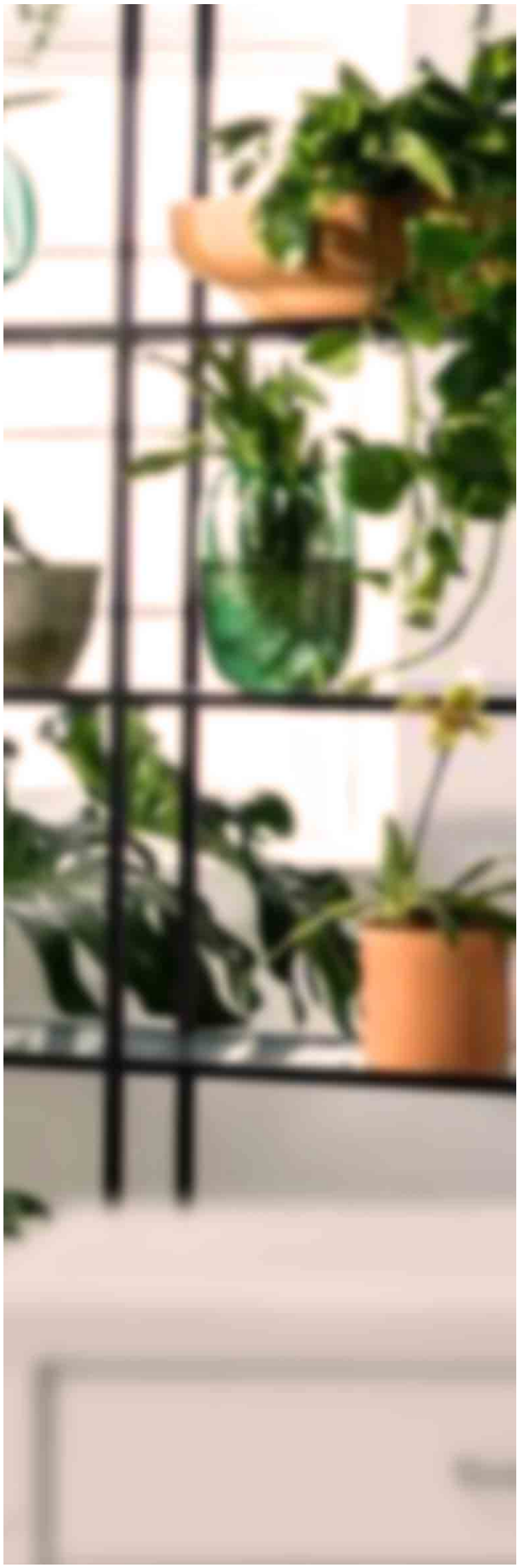
En general, el ciberbullying tiene características propias:

- La viralización: los chicos en general no tienen noción sobre el alcance que puede tener una publicación dado que, como se señaló antes, Internet produce una circulación constante de información que puede generar que desconocidos o personas ajenas al grupo donde se realiza la acción accedan al contenido difundido.

- Rapidez: la circulación de la información se produce en segundos, por lo que no sólo se expande por toda la red sino que lo hace a gran velocidad.

- La sensación de anonimato: al llevar adelante la acción mediante un dispositivo, se crea una sensación de anonimato que genera la creencia de minimizar la agresión.





¿CÓMO PUEDO APRENDER MÁS SOBRE PROTECCIÓN DE DATOS Y PRIVACIDAD EN INTERNET?

Desde 2014, la Defensoría, a través de su Centro de Protección de Datos Personales y del Observatorio de Derechos en Internet, lleva adelante el programa “Conectate Seguro” sobre uso seguro de las Tecnologías de la Información y la Comunicación, donde se abordan temas de protección de datos personales y privacidad en Internet.
Si querés que vayamos a tu escuela, centro de jubilados o a tu barrio escribinos a cpdp@defensoria.org.ar o a dei@defensoria.org.ar

¿QUÉ LEYES ME PROTEGEN?

En relación con nuestros datos personales, además del artículo 43 de la Constitución Nacional, existen leyes que garantizan derechos frente al tratamiento de esa información almacenada en bases de datos por parte del Estado o del sector privado. Lo que aquí se quiere resaltar es que estas leyes se aplican tanto a las bases de datos físicas (ficheros) como a las bases digitales.
Las leyes son:

- Ley nacional 25326 de Protección de Datos Personales, que tiene por objeto la protección de los datos personales asentados en bancos de datos u otros medios técnicos de tratamiento de datos, sean estos públicos o privados destinados a dar informes.
- Ley porteña 1845 de Protección de Datos Personales, que tiene por objeto regular, dentro del ámbito de la Ciudad de Buenos Aires, el tratamiento de datos personales asentados o destinados a ser asentados en bases de datos del sector público de la Ciudad de Buenos Aires.

Entre algunos de los derechos consagrados en la ley se encuentra el derecho a información, acceso, rectificación, actualización y supresión de datos personales.

¿QUÉ ES EL *GROOMING*?

El grooming es la acción deliberada de un adulto de contactar a un niño o niña a través de distintos canales de Internet para ganar su confianza con el fin de acosarlo sexualmente.
Estos adultos suelen crear un perfil falso en una red social o sala de chat haciéndose pasar por un chico o una chica, y entablan una relación de amistad y confianza con la persona que quieren acosar.
Una vez que se establece esta relación de confianza, el adulto –siempre haciéndose pasar por un menor– suele pedir una foto o video con contenido sexual y, ya en poder de ese material, comienza un periodo de extorsión en el que se amenaza al niño o niña con hacerlo público si no accede a un encuentro personal.
En nuestro país, desde 2013 el grooming encuentra regulación en el Código Penal (Ley 26904) con una pena de hasta 4 años de prisión por considerarse una práctica preparatoria para un abuso sexual.

■ **Antivirus:** programa cuya finalidad es prevenir los virus informáticos, así como curar los ya existentes en un programa.

■ **Aplicación:** cualquier programa que corra en un sistema operativo (por ejemplo, Android o IoS) y que brinde una función específica para un usuario.

■ **Blog:** es una herramienta online para que el usuario pueda subir información a un sitio web en forma sencilla e instantánea.

■ **Contraseña:** código utilizado para acceder a un sistema restringido.

■ **Correo electrónico o e-mail:** permite el intercambio de mensajes entre las personas conectadas a la Red. Para ello es necesario tener una dirección de correo electrónico.

■ **Facebook:** una de las redes sociales con más usuarios del mundo. Permite estar en contacto con "amigos", ver la información que los mismos u otros usuarios hayan puesto en el muro, estar actualizado con las novedades de ciertos productos o servicios. Así como también es utilizado para promocionar todo tipo de negocios y marcas.

■ **Googlear:** acción de buscar cualquier tipo de información en el buscador más popular de Internet, o sea, Google.

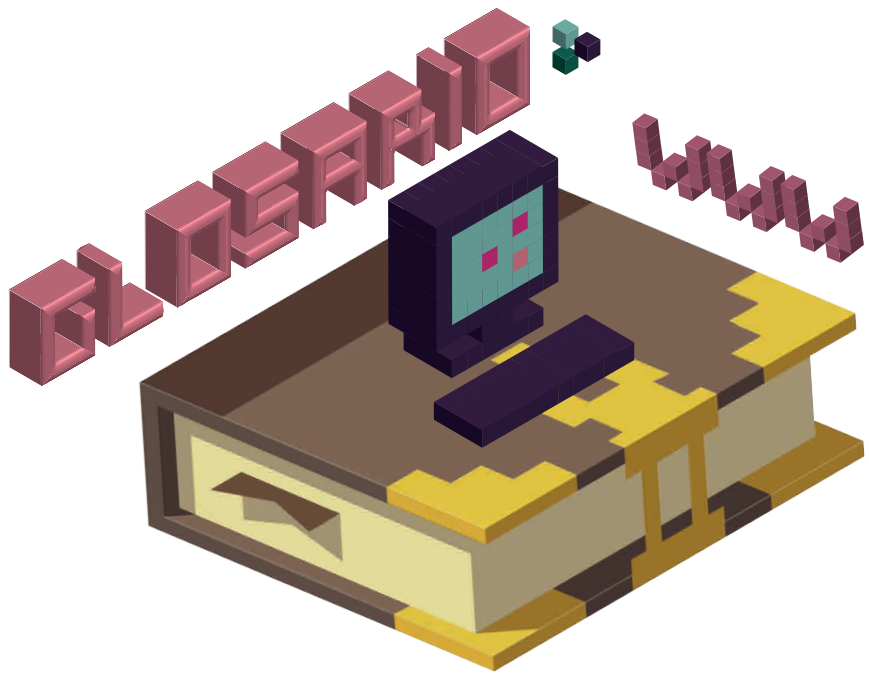
■ **HTTP:** es protocolo utilizado para el intercambio de información a través de la World Wide Web (WWW).

■**HTTPS:** es el protocolo anterior donde, por estar cifrada la información intercambiada, la circulación se realiza de forma segura.

■ **Instagram:** es una red social que permite tomar o subir fotografías ya tomadas, modificarlas con efectos especiales para luego compartirlas con otras personas en su plataforma o en otras redes sociales.

■ **Muro:** dentro de una red social, se trata de un espacio individual dentro de cada usuario donde aparecen sus actualizaciones y diversos posteos.

■ **Nube:** son los servidores donde se aloja información tal como bases de datos, correo electrónico o gestión de recursos humanos.



■ **Perfil:** es el nombre que recibe cada cuenta individual y personal de quienes usan alguna red social.

■ **Postear:** acción de subir algo, ya sea una foto, un video, un link o escribir algo en una página de Internet para que otros lo vean.

■ **Protocolo TCP/IP:** representa las reglas que hacen posible la conexión de computadoras de marcas y tecnologías diferentes. Fue creado a principios de los '80 con la finalidad de contar con un lenguaje común a todas las computadoras conectadas a Internet.

■ **Redes sociales:** son plataformas que permiten la fácil interacción entre personas por medios digitales.

■ **Servidores:** equipamiento informático, a gran escala, destinado a alojar archivos de páginas web.

■ **Snapchat:** es una aplicación móvil dedicada al envío de mensajes en forma de fotos o vídeos de corta duración. Los usuarios pueden controlar el tiempo que los mensajes serán visibles, tras lo cual desaparecerán del servidor. Tiene una modalidad dentro de la aplicación llamada "snapcash" que permite habilitar el envío de dinero.

■ **Streaming:** es la tecnología que nos permite ver un archivo de audio o video directamente desde Internet. Además, ver u oír transmisiones en vivo y en directo a través de reproductores específicos.

■ **Telegram:** es un servicio que permite enviar y recibir mensajes (texto, documentos, imágenes, vídeos, archivos de gran tamaño, etc.) y donde el énfasis está puesto en la privacidad y la seguridad de la información. Para lograrlo permite la creación de "chat secretos" que establecen una conversación discreta y efímera cuyos mensajes son cifrados desde el dispositivo y solo son recibidos por el emisor que tenga la clave.

■ **TIC:** siglas correspondientes a las Tecnologías de la Información y Comunicación. Son herramientas / tecnologías que permiten el almacenamiento, intercambio y todo tipo de procesamiento de la información.

■ **Twitter:** es la red social en donde los usuarios que están registrados pueden escribir lo que quieran, pero cada mensaje o "tweet" tiene un límite de caracteres (actualmente 140). La idea es generar mensajes cortos. Ya no se habla de "amigos", como en el Facebook, sino de "seguidores".

■ **Virus:** se trata de un programa malicioso que ingresa en la computadora creando inseguridad y riesgo para los datos allí guardados / almacenados.

■ **Whatsapp:** servicio de mensajería instantánea que permite intercambiar audios, imágenes, archivos y ubicación.

■ **Wi-Fi:** se trata de una red inalámbrica que transmite datos en banda ancha en un determinado rango.

¿LA DEFENSORÍA DEL PUEBLO PUEDE AYUDARME?

Si tenés alguna duda o reclamo en relación a la protección de tus datos personales en general, podés contactarte con el Centro de Protección de Datos Personales y Observatorio de Derechos en Internet de la Defensoría llamando de lunes a viernes de 10 a 18 al 0800-999-3722, enviando un correo-e a cpdp@defensoria.org.ar o concurriendo personalmente a cualquiera de las sedes de la Defensoría.

EN INTERNET, TENÉS LOS MISMOS DERECHOS.

SEDES

Monserrat
Av. Belgrano 673

Flores
Carabobo 84

Parque Patricios
Guaraní 242

Colegiales
Delgado 771

Lacroze
Federico Lacroze 2751

Retiro
Puente 1 de la Terminal de Ómnibus
Local 36

Plaza Miserere
Estación del mismo nombre de
la línea A de subtes

Constitución
Subsuelo de la estación de trenes
Local 60 B

Floresta
Sanabria 2440

Villa 21.24
Casa de la Cultura
y Capilla de Caacupé

Santa Fe
Santa Fe 1736

Villa 20
Pola y Barros Pazos

CAJ Once
Av. Rivadavia 2690

CAJ Constitución
Salta 2007

Villa 31
Calle 5 y Calle 10

Mataderos
Emilio Castro 7680

Rodrigo Bueno
Centro Comunitario R. Bueno, Boulevard Elvira
R. de Dellepiane y Av. España, Manzana 3

Los Piletones
Lacarra y Ana María Janer

Playón de Chacarita
Fraga 900-Capilla Sagrado Corazón

Defensoría LGBT
(Lesbianas, Gays, Bisexuales y Trans)
Avenida de Mayo 881 2° piso "J"

AMIA
Pasteur 633

Villa 1.11.14
Parroquia Madre del Pueblo
Avenidas Perito Moreno y
Fernández de la Cruz
Manzana 3-Casa 1

Defensoría del Turista

Monserrat
Piedras 445

San Telmo
Defensa 1250

San Telmo II
Defensa 1302

La Boca
Av. Pedro de Mendoza 1835
(Museo Benito Quinquela Martín)

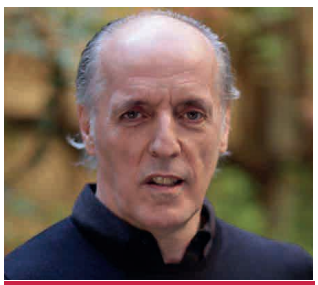
Terminal de Cruceros
Av. Ramón Castillo y Av. De los Inmigrantes

Recoleta
Pte. Juan Manuel Quintana y Pte. R. M. Ortiz

Palermo
Beruti 3345

Florida
Florida y Marcelo T. de Alvear

Puerto Madero
Av. Alicia Moreau de Justo 200 (Dique 4)



ALEJANDRO AMOR
Defensor del Pueblo de la Ciudad Autónoma de Buenos Aires

LA PROTECCIÓN DE TU IDENTIDAD DIGITAL

Las formas de la sociabilidad contemporánea se ven constantemente modificadas por los avances tecnológicos y las nuevas modalidades de comunicación e interacción. En este sentido, es necesario reflexionar sobre la relación entre la tecnología y el manejo de la información personal y privada. Debemos reconocer que los dispositivos comunicativos son buenos y útiles siempre y cuando sean utilizados con conciencia. Para ello debemos capacitar y educar especialmente a los niños, niñas y adolescentes en el uso de herramientas como Internet de una manera integral, tomando en cuenta también la protección de sus datos personales. Debemos hablar con ellos sin tabúes, enseñarles a preservarse y a avisar si están ante una situación de acoso o que consideran peligrosa.

En este sentido, el Centro de Protección de Datos Personales de la Defensoría del Pueblo viene realizando en diferentes instituciones educativas el programa “Conectate Seguro” en donde se abordan cuestiones vinculadas al uso de las TIC, Internet y redes sociales. Pero ante la realidad, necesitamos redoblar esfuerzos. Por eso proponemos que la guía de protección de los derechos de los usuarios de Internet que presentamos en esta oportunidad sirva para ayudarnos a pensar en conjunto a adultos y a jóvenes en cómo hacer para evitar más casos de acoso, violencia y maltrato virtuales que, muchas veces, traspasan las fronteras y modifican la realidad de las personas de manera brutal.

La prevención no se logra solo con información. Debemos entender el porqué de las cosas, como adultos debemos enseñar a los jóvenes a valorar su identidad, cuidarse y también cuidar a los demás. Te invito a vos a que hables con tus amigos y amigas, con tus familiares, tus hijos, vecinos, incluso hasta con tus amigos virtuales para generar vínculos reales, de cuidado y protección.

Si fuiste víctima o sabés de alguien que esté siendo víctima de acoso virtual, denuncialo en la Defensoría. Tenés quien te defienda.

@DefensoriaCABA DefensoriaCABA
www.defensoria.org.ar

Atención al Vecino Av. Belgrano 673
0800 999 3722

Defensoría del Pueblo
Ciudad Autónoma de Buenos Aires