Infojus
SISTEMA ARGENTINO DE INFORMACIÓN JURÍDICA

con vos en la web

PDP

Guías para adultos: desafíos y riesgos en el mundo digital

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

PRESIDENCIA DE LA NACIÓN
Dra. Cristina Fernández de Kirchner

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
Dr. Julio Alak

SECRETARÍA DE JUSTICIA
Dr. Julián Álvarez

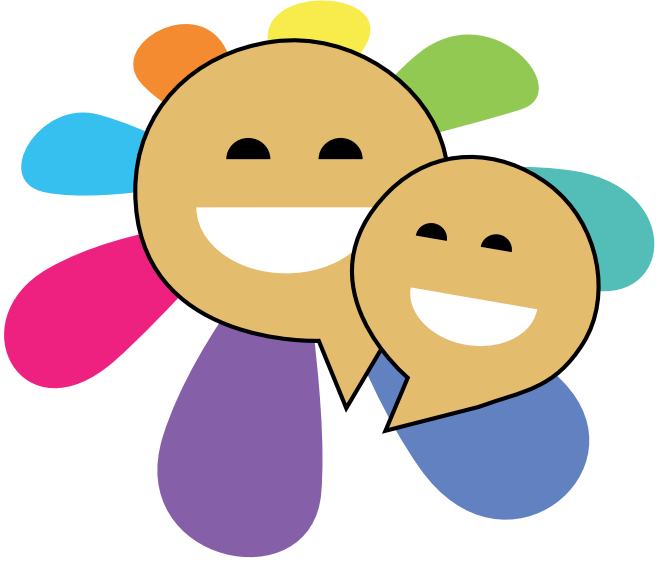
SECRETARÍA DE ASUNTOS REGISTRALES
Dr. Oscar Martini

SUBSECRETARÍA DE COORDINACIÓN Y CONTROL DE GESTIÓN REGISTRAL
Dr. Ernesto Kreplak

DIRECCIÓN NACIONAL DE PROTECCIÓN DE DATOS PERSONALES
Dr. Juan Cruz González Allonca

COORDINACIÓN DEL PROGRAMA CON VOS EN LA WEB
Lic. Ezequiel Passeron

Introducción



La irrupción tecnológica sin precedentes vivida en los últimos años generó cambios y desafíos que requieren herramientas y estrategias específicas. Nuevas formas de comunicación, información, diversión y educación modificaron las vidas de grandes y chicos. En este escenario, el rol del adulto se ve interpelado y cuestionado. ¿Están capacitados los adultos para acompañar a los niños, niñas y adolescentes en la web? ¿Es necesario que los acompañen? El presente documento tiene como objetivo describir las principales temáticas, riesgos y problemas que surgen del uso de las nuevas tecnologías y plantear la importancia del acompañamiento adulto en la vida digital de los chicos.

El material presentado a continuación es la recopilación del trabajo realizado por 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. Con Vos en la Web es un Programa de educación sobre uso responsable de las nuevas tecnologías. Su objetivo es generar herramientas para que los jóvenes y los adultos eviten riesgos y construyan una ciudadanía digital respetuosa. Para cumplir con sus objetivos, Con Vos en la Web realiza talleres para chicos y capacitaciones para adultos en todo el país. En el mismo sentido, el Programa ofrece diversos contenidos: guías, videotutoriales, consejos y aplicaciones móviles. A raíz del trabajo junto con Conectar Igualdad, Unicef, Argentina Conectada, Educ.ar, entre otros, Con Vos en la Web, profundizó su trabajo, federalizó su iniciativa y capacitó a miles de chicos y adultos en todo el país. Con una mirada positiva sobre la web, y con el objetivo de evitar problemas y potenciar el respeto hacia el otro, fomenta el uso de herramientas tecnológicas.

Cyberbullying, grooming, reputación digital, amenazas web, uso seguro de Wi-Fi y derechos sobre los datos personales en Internet, son las principales temáticas trabajadas por Con Vos en la Web. Estas han sido volcadas en el presente documento, que tiene como fin que los adultos, en sus diversos roles, conozcan, prevengan, gestionen y acompañen a los chicos.

Infojus

Infojus

Protección de datos personales

La Ley y todo lo que tenemos que saber para ejercer nuestros derechos

La Ley de Protección de los Datos Personales asegura la protección integral de los datos personales. Su función es garantizar el derecho al honor y a la intimidad de las personas, y regular el acceso a la información que sobre las mismas existe.

Con la llegada de las Tecnologías de la Información y la Comunicación —TIC—, Internet y las redes sociales, se multiplica el desafío para la correcta protección de los datos personales. Así, vemos cómo en Facebook, Twitter, YouTube, Instagram, Flickr, o bien en blogs, se publican nombre, apellido, fecha de nacimiento; se suben las fotos más personales y hasta se publican datos sensibles como ideología política, creencias religiosas, etc.

El objetivo de esta publicación es establecer pautas que desarrollen capacidades críticas y reflexivas en sus principales usuarios —los niños y jóvenes— respecto del uso de las nuevas tecnologías y, a su vez, orientar a padres y docentes para que acompañen a los más chicos en este desafío.

Los chicos comparten cada vez más información y lo harán en el futuro. Es prioritario entender a la gestión de la privacidad como una nueva competencia a aprender, enseñar y proteger. Por esto es que debemos profundizar la aplicación de leyes como la de Protección de los Datos Personales (ley 25.326), que nos permitan seguir construyendo más ciudadanía y mejor calidad de vida para los niños, niñas y adolescentes de la Argentina.

Ernesto Kreplak,
Subsecretario de Coordinación
y Control de la Gestión Registral

¿Cómo cuidar nuestros datos?

¿Se sabe que existe una ley nacional que tiene como objetivo la protección de los datos personales para garantizar el derecho a la privacidad y a la intimidad?

La Dirección Nacional de Protección de Datos Personales (PDP) es la oficina que brinda asesoramiento y ayuda para la protección de los datos personales. Su trabajo es ofrecer colaboración para que entendamos los derechos que nos da la Ley de Protección de los Datos Personales (ley 25.326) y conozcamos la forma de ejercerlos.

¿Qué son los datos personales?

Los datos personales son cualquier tipo de información que se relacione con nosotros y nos identifique: nombre y apellido, número de documento, domicilio, dirección de correo electrónico, usuario y fotos o videos de Facebook, grabaciones de voz, huellas digitales, tweets, etc.

Un tipo especial de datos personales son los datos sensibles. Estos demandan mayor protección porque se relacionan con temas delicados, que pueden afectar los sentimientos, como: origen, opiniones, creencias e información sobre la salud o la sexualidad de las personas.

Puede ser que una página web o una red social, por ejemplo, tenga un registro con muchos de nuestros datos personales, los que pueden ser usados de distintas formas, pudiendo ser recolectados, conservados, ordenados, destruidos o entregados a otros.

¿Por qué es necesario protegerlos?

El cuidado de los datos personales es importante ya que existen riesgos y amenazas (robo de identidad, estafas, uso indebido de tus datos, etc.) que pueden representar peligros para nosotros, nuestra familia y amigos.

¿Quién es "dueño" de sus datos personales?

¡Cada uno de nosotros!

Todas las personas son titulares o "dueños" de sus propios datos personales. Entonces, solo ellas deberían decidir qué información suya quieren que los demás conozcan.

Podemos entregar datos personales a otras personas para que los usen con una determinada finalidad. Por ejemplo, podemos darle datos sobre nuestra salud a nuestro médico para que nos cure, pero es importante saber que no puede usarlos para otro fin.

¿Cómo protege esta ley nuestros datos personales?

Derecho de información

Nos permite saber qué datos sobre nosotros tiene una empresa, por ejemplo. Para averiguarlo, se puede consultar con la Dirección Nacional de Protección de Datos Personales (PDP), donde se brindará toda la información de contacto de esa empresa.

Ello es posible porque la Dirección Nacional de Protección de Datos Personales (PDP) posee el Registro Nacional de Bases de Datos, en el cual tienen que inscribirse todas las personas, empresas u organismos públicos que tienen bases de datos que excedan el uso privado.

Derecho de acceso

Nos permite conocer la información sobre cada uno de nosotros que está disponible en una base de datos. Con solo demostrar nuestra identidad, tenemos el derecho a obtener información acerca de qué datos personales están incluidos en las bases de datos públicas o privadas.

El responsable del Registro Nacional de Bases de Datos debe darnos la información pedida, que tiene que ser clara y estar expresada en un lenguaje fácil de entender.

Derecho de rectificación o actualización

Si nuestros datos personales están anotados en forma incorrecta en una base de datos, tenemos derecho a pedir que sean corregidos o actualizados de manera gratuita, o que no se den a conocer a otras personas.

Derecho de supresión

Podemos solicitar que, en forma gratuita, se elimine información sobre nosotros que sea falsa o esté disponible sin autorización o por error.

En la Dirección Nacional de Protección de Datos Personales se puede obtener asesoramiento gratuito por vía telefónica o en persona para que podamos ejercer estos derechos.

Infojus

¿Cómo hacer para autorizar el uso de los datos?

Para que alguien pueda usar nuestros datos personales, tenemos que dar autorización o consentimiento. Si no lo hacemos y los datos son usados igual, ese uso de nuestros datos personales es ilegal.

Es muy importante que, antes de dar autorización, estemos muy bien informados acerca de para qué serán usados y de quiénes tendrán acceso a ellos. Es necesario que nos aseguremos de que se respete la finalidad para las que autorizamos el uso de nuestros datos. Por ejemplo: una red social no puede vender los datos sobre las cosas que nos gustan a empresas que venden esas cosas si no nos avisaron que estaban recolectando los datos para tal fin.

En el caso de los menores de 18 años, los padres pueden dar autorización para el uso de los datos personales de su hijo/a. Solo en algunos casos no es necesaria la autorización: si los datos usados incluyen solo el nombre, DNI, ocupación, fecha de nacimiento y domicilio; si son datos que están en bases de datos públicas, como la guía telefónica; o si se trata de datos que tiene el Estado, como los datos de nacimiento que tiene el Registro Civil o aquellos que tiene el Ministerio de Educación sobre los alumnos de escuelas públicas.

Más sobre los datos sensibles

Nadie puede obligarnos a proporcionar datos sensibles. Solo pueden ser recolectados y usados cuando lo autorice una ley o cuando se usen para hacer estadísticas o investigaciones científicas y no se identifique a la persona por su nombre, documento o foto.

Está prohibido hacer bases de datos sensibles. Pero, por ejemplo, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales están autorizadas a llevar un registro de sus miembros.

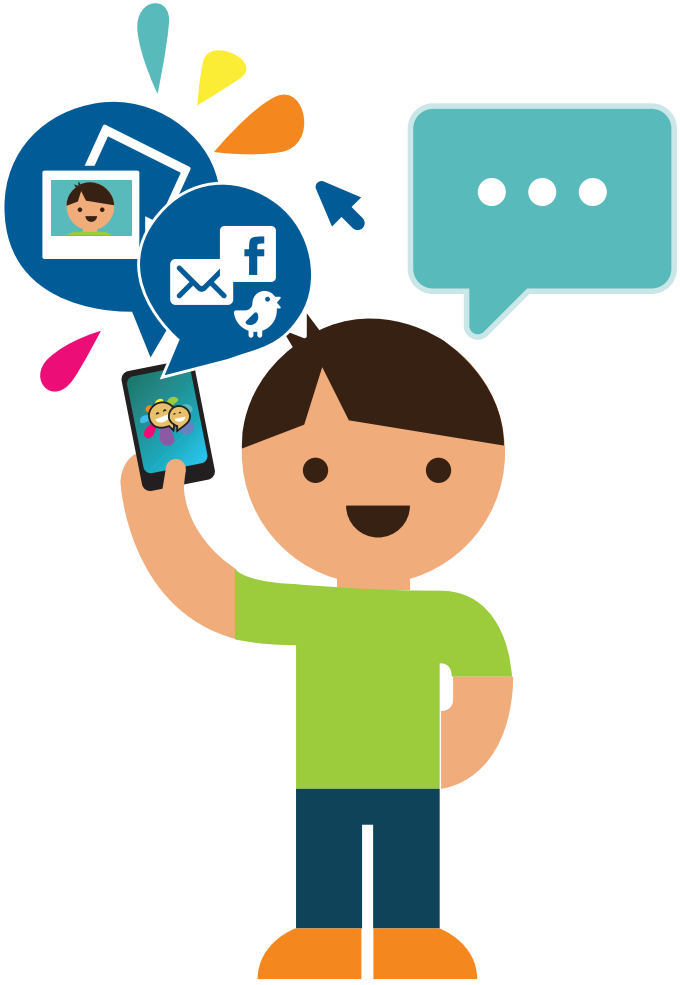
Los datos relativos a antecedentes penales o contravencionales (infracciones que no llegan a ser un delito penal) solo pueden ser tratados por las autoridades públicas, como la Policía.

Los datos sobre la salud solo pueden ser usados por los hospitales y por los profesionales de la salud. Los médicos, odontólogos, enfermeros, etc., pueden usar tales datos bajo la condición de respetar siempre el principio del secreto profesional.

Publicidad

Está permitido que nos envíen mails o nos llamen por teléfono ofreciéndonos productos o servicios, porque tomaron nuestros datos de una base accesible al público, como la guía telefónica, o bien porque se les dimos para que nos contacten. Sin embargo, tenemos derecho a pedir, en cualquier momento, que saquen nuestro nombre de esa base y no nos sigan ofreciendo esos productos y servicios.

Reputación Web



¿Qué es?

La reputación web es la imagen, el prestigio y la referencia sobre nosotros mismos que se genera a raíz de información que subimos a Internet: publicaciones, fotos y videos.

Internet es, en la actualidad, la principal fuente de información y comunicación. En ese sentido, los datos en la web que se asocian a nuestro nombre se convertirán en la manera que tengan terceros para conocernos más.

¿Qué incluye?

Los posteos que publiquemos o donde nos etiqueten; las fotos o los videos subidos por nosotros o por terceros donde estemos nombrados; los blogs o los sitios web donde citen nuestro nombre o donde firmemos producciones propias; y los registros de participación en foros, juegos o redes sociales son algunas de las fuentes que crean nuestra reputación web.

¿Cómo se construye?

Variados son los modos en los que se va armando la reputación web. Esta puede construirse por acción propia, por acción de terceros e, incluso, por omisión.

Acción propia

Consiste en las publicaciones que hacemos en redes sociales, blogs, sitios web o foros aclarando nuestra identidad.

Acciones de terceros

Consiste en las publicaciones hechas por otros, en donde nos citan o nombran.

Omisión

Ante el impacto de Internet, no tener cuentas en redes sociales o participación web es, de por sí, un dato que se incluye en nuestra reputación cuando alguien busca información sobre nosotros.

¿Se puede modificar o borrar?

La reputación se construye a lo largo de años y es difícil de borrar o modificar ya que en Internet no hay olvido.

Si bien se puede pensar que, al borrar una publicación, estamos eliminando la totalidad de esa referencia, es importante recordar que otra persona puede haber descargado, compartido o guardado el posteo o el contenido y, por ende, volver a subirlo y compartirlo. Allí estaríamos perdiendo el control de nuestro dato personal.

¿Por qué alguien guardaría una publicación que nosotros quisimos borrar? Por diversos motivos, que pueden ser tanto personales (broma o venganza, por ejemplo) como propios de la estructura de la web.

La dinámica de Internet genera que algunos contenidos comiencen a ser compartidos rápidamente por distintos usuarios; este proceso es llamado "viralización".

Un contenido puede viralizarse por ser gracioso, polémico, atractivo, de denuncia o por otras razones. En la mayoría de los casos es difícil prever su viralización y alcance, pudiendo llegar a cientos, miles o hasta millones de personas.

Para aprender a configurar la privacidad de todas las cuentas, podemos ver los video tutoriales del sitio web www.convosenlaweb.gob.ar

Resulta relevante considerar que la multiplicidad de plataformas que nos ofrecen las nuevas tecnologías hace que nuestra información rápidamente se viralice a través de distintos dispositivos o redes (PC, tablets, smartphones, chats, redes sociales, etc.).

Es importante pensar que un contenido que querramos borrar puede haber tenido un sentido imprevisto para una persona que lo descargó, quien puede compartirlo en su formato original o, incluso, después de haberlo modificado. Esto quiere decir que se puede mantener nuestra foto, video o comentario, pero editar y modificar lo que pusimos para compartirlo con desconocidos. En esos casos, perderemos el poder de borrarlo e impedir que forme parte de nuestra reputación web.

¿Por qué nos importa la reputación web?

En la actualidad, Internet es la principal forma de conocer a una persona. A continuación, detallamos algunos casos donde la reputación web se vuelve importante:

Búsqueda laboral

Si bien cuando buscamos o nos presentamos en una entrevista laboral presentamos un currículum vítae armado por nosotros, la penetración de Internet en la vida cotidiana hará que nuestro futuro jefe o entrevistador busque referencias de nuestro perfil en la web. Para hacerlo, pondrá nuestro nombre en los buscadores y analizará todas las referencias que aparezcan. Si no configuramos nuestra privacidad en Facebook, Twitter u otra red social, la primera respuesta del buscador será nuestro perfil en esa red social, por lo que podrán indagar en las publicaciones que hicimos desde que abrimos la cuenta. Muchas veces, subimos material vinculado a cuestiones privadas y que solo tienen sentido en relación a un contexto específico. Por ende, visto fuera de él y por un posible jefe, puede perder sentido y ser incorporado como algo negativo a la hora de evaluar nuestra incorporación.

Cita

Cuando conocemos a alguien, solemos contar quiénes somos, qué nos gusta y qué no nos gusta, durante la charla personal. Si la persona con la que nos encontramos nos busca en la web, puede ver información privada o íntima que preferiríamos que no sepa en un primer encuentro.

Referencias

Cuando nos encontramos con alguien para realizar intercambios profesionales o personales, lo más probable es que esa persona nos busque en la web para conocernos más. De esta forma, puede ocurrir que se encuentre con información de índole personal que puede generar un prejuicio sobre nuestro perfil o personalidad. Si queremos elegir cómo mostrarnos, la reputación web es indispensable.

¿Qué riesgos corremos si no cuidamos nuestra reputación web?

- Que brindemos información privada, actual o del pasado, a personas que no tendrían por qué recibirla.
- Que nos encasillen o estereotipen con información que tiene sentido en un ámbito (privado), pero que lo pierde en otro (público).
- Que nuestra trayectoria o imagen se vea empañada por información pasada o brindada por terceros. Este tipo de información, que puede ser tanto antigua como errónea, quedará asociada a nuestro nombre en cada búsqueda que se realice para conocernos más.
- Que adelantemos información que comúnmente brindamos cuando conocemos con mayor profundidad a alguien y que, por ello, corramos el riesgo de quemar etapas en relaciones tanto profesionales como personales.
- Que se nos relacione con actividades o actitudes pasadas o erróneas, que afecten la opinión de quien nos busque y actúen como filtros de selección que nos quiten la oportunidad de presentarnos en forma personal.

¿Cómo cuidar nuestra reputación web?

1. Configuremos la privacidad en las redes sociales para establecer que solo nuestros contactos tengan la posibilidad de ver nuestras publicaciones, tanto del pasado como del presente. De esta forma evitaremos que desconocidos tengan acceso a nuestros posteos, fotos o videos.
2. En caso de agregar a desconocidos a nuestras redes sociales, debemos tener mayor cuidado en la información que publicamos ya que esa persona puede tener intenciones igualmente desconocidas respecto de nuestros datos e intentar reproducirlos.
3. Pensemos antes de publicar. Tengamos siempre en cuenta que en Internet no existe el olvido y que, por ende, podemos perder el control sobre lo subido.
4. Controlemos qué información sobre nosotros circula en Internet. Herramientas como "Google alerts" pueden avisarnos que fuimos nombrados e informarnos cada vez que ello suceda. También es un buen ejercicio escribir nuestro nombre en los buscadores y así saber qué se dice en la web sobre nosotros.
5. Coloquemos contraseñas en nuestros celulares para evitar que otras personas accedan a la información, fotos, videos o a los mensajes que guardamos en nuestros teléfonos móviles. Esa persona puede querer publicar, por diversos motivos, esa información privada en la web y afectar nuestra respectiva reputación.
6. Utilicemos contraseñas seguras, fáciles de recordar pero difíciles de adivinar; además, no las compartamos y modifiquémolas periódicamente. Nuestras computadoras, celulares, cuentas en redes sociales, blogs, foros o correos electrónicos contienen información que debemos cuidar. Si caen en manos de otras personas, pueden publicar algo que no elegiríamos hacer público.
7. Recordemos siempre que cada uno de nosotros es el dueño de sus datos y elijamos a quién y cuándo damos información personal.
8. Tengamos en cuenta que los amigos *online*, por más cariño que nos despierten, son desconocidos. Eso no significa que tengamos que dejar de hablarles, pero sí que debemos cuidar la información personal que les damos, ya que pueden difundirla o publicarla.
9. Evitemos colocar nuestro nombre y apellido en las producciones o publicaciones que no deseamos que se asocien a nuestra identidad. En estos casos, es recomendable utilizar seudónimos.

Cyberbullying

Información y consejos para entender y prevenir el acoso 2.0

¿Qué es?

El ciberacoso puede definirse como la acción de llevar a cabo "amenazas, hostigamiento, humillación u otro tipo de molestia realizadas por un adulto contra otro adulto por medio de tecnologías telemáticas de comunicación, es decir: Internet, telefonía móvil, correo electrónico, mensajería instantánea, juegos *online*, redes sociales, etc".(1)

El cyberbullying es un caso de ciberacoso aplicado en un contexto en el que únicamente están implicados niños, niñas y adolescentes, y supone uso y difusión de **información de datos difamatorios y discriminatorios a través de dispositivos electrónicos** como correos, mensajería instantánea, redes sociales, mensajería de texto o **la publicación de videos o fotos**.

La discriminación es tal, tanto en el espacio *online* como en el *offline*. Por ende, "es discriminatoria toda distinción, restricción, o preferencia basada en motivos de una supuesta raza, religión, nacionalidad, ideología, opinión política o gremial, sexo, posición económica, condición social o caracteres físicos que tenga por objeto anular o menoscabar el reconocimiento y ejercicio en condiciones de igualdad de los derechos humanos y libertades fundamentales en las esferas políticas, económicas, sociales, culturales o en cualquier otra esfera de la vida pública".(2)

(1) Aftab, Parry, *Cyberbullying: Guía práctica para madres, padres y personal docente,* Jorge Flores y Manu Casal (adaptación y contextualización), Bilbao, Edex, 2006.

(2) Instituto Nacional Contra la Discriminación, la Xenofobia y el Racismo (INADI), "¿Por qué?", [en línea] http://internet.inadi.gob.ar/por-que

Características

Si bien el cyberbullying tiene grandes semejanzas con el bullying, es importante que conozcamos los rasgos propios de este tipo de acoso para reconocer sus reales dimensiones y particularidades.

Viralización

Los chicos y chicas en muchos casos no tienen noción sobre el alcance que puede tener una publicación. Internet produce una expansión de contenidos capaz de provocar que desconocidos o personas ajenas al grupo primario accedan a la publicación realizada.

Cuando se sube una información, se pierde el control sobre quién lo comparte o guarda y, por ende, acerca de cuántas personas conocen lo que decimos sobre otro. Esto causa mayor perjuicio en el acosado ya que la información difamatoria puede viralizarse fuera del círculo conocido, potenciando el daño a la imagen.

Ausencia de olvido

Internet no ofrece el derecho al olvido y, por ende, aunque se borre lo publicado, si otra persona ya guardó la información, esta seguirá reproduciéndose.

Además, los registros de navegación guardan datos, lo que genera que no haya seguridad sobre la desaparición de la información. Esto conduce a que el daño causado sobre quien sufre el acoso no tenga un final establecido y continúe reproduciéndose.

Falsa sensación de anonimato

Internet puede invitar a participar del acoso a personas por parte de quienes no lo harían en forma personal. La falsa sensación de anonimato genera una también falsa sensación de minimización de la agresión, cuya consecuencia es que más personas se sumen al cyberbullying, agrandando el círculo de discriminadores.

Existencia de diversos dispositivos para el hostigamiento

La web ofrece medios variados para realizar el acoso, como cadenas de mails, mensajes personales y divulgación de imágenes o videos difamatorios. Esto reduplica el daño, ya que pueden combinarse los dispositivos y, por ende, multiplicarse los canales de difusión y recepción.

Falta de registro del otro

La agresión personal tiene como característica la respuesta inmediata del agredido. En la llevada a cabo en la web, en cambio, no contamos con la información sobre cómo lo que publicamos lastima al otro en forma inmediata, lo que puede motivar la profundización de la la humillación. Si en una pelea el agresor se da cuenta de que el agredido se siente herido, es posible que se arrepienta o interrumpa su acción. La web impide ver los gestos o la reacción del otro y, por ello, es probable que la agresión se extienda a pesar de que implica lastimar al otro.[3]

Perfiles

Los perfiles de los discriminadores, cuando se extienden a Internet, se modifican y hasta pueden invertirse. Es importante que sepamos que los clásicos perfiles de los agresores no se copian en la web, sino que nuevas personas pueden verse tentadas a participar, tanto produciendo como compartiendo información. La falsa sensación de anonimato, sumada a la soledad en la que suele establecerse la conexión, permite que quienes no se animan a discriminar en forma personal, tengan más facilidades para hacerlo vía web. El referido libro *Cyberbullying: Guía práctica para madres, padres y personal docente,* publicado en España, tipifica los perfiles existentes en el acoso por web. Aquí nos proponemos desarrollarlos para entender todas sus dimensiones.

El acosador

Persona que, generalmente por problemas de autoestima, necesita manifestar su poder humillando a otro.

La víctima

Persona que sufre la humillación o discriminación. Las características propias de Internet conducen a

(3) Aftab, Parry, *op. cit.*

que, más allá de cualquier timidez, tenga mayores posibilidades de venganza que en la vida *offline*. Es por eso que es importante no responder con más violencia a la discriminación.

Los espectadores

Aquellos que ven la agresión "desde fuera". Pueden convertirse en eventuales alentadores del hecho o asumir el rol de sujetos pasivos. Sin embargo, en Internet, el espectador cobra otro protagonismo ya que tiene la posibilidad de compartir información. Es importante que sepamos que compartir también es participar y que, por ello, no hacerlo es cortar el círculo de la humillación y, por lo tanto, una forma de ayudar.

El reforzador de la agresión

Aquel que estimula al agresor. En la web, puede potenciar el alcance de la información humillante y, por ende, cobra un gran protagonismo. Es un tipo de perfil que pasa a un primer plano en el cyberbullying.

El ayudante del agresor

Persona que coopera con el agresor. Si bien en la web puede cumplir el mismo rol que el reforzador, su perfil cobra un protagonismo mayor porque puede extender el alcance de lo público.

Es importante en ambos casos reforzar la idea de que no solo quien produce la información es el agresor, sino también quien comparte y potencia la publicación.

El defensor de la víctima

Aquel que intenta ayudar al agredido a salir de su victimización.

Formas de cyberbullying

La discriminación web puede volcarse o expresarse en distintas formas.[4] Por lo tanto, es necesario que las conozcamos para poder prevenirlas y gestionarlas.

Hostigamiento

Envío de imágenes denigrantes; seguimiento a través de software espía; envío de virus informáticos; selección de jugadores en los juegos *online* para la humillación de otro por su forma de juego, entre otros.

Exclusión

Uso de entornos públicos para acosar y mandar comentarios despectivos o difamatorios con el objetivo de provocar una respuesta expansiva; denegación del acceso a foros, chats o plataformas sociales de todo el grupo a la víctima, entre otros.

Manipulación

Uso de información encontrada en las plataformas para difundirla de forma no adecuada entre los miembros; acceso con la clave de otra persona a un servicio y realización de acciones perjudiciales en su nombre, entre otros.

Consecuencias

Cualquier tipo de discriminación lleva como principal consecuencia la humillación para el agredido. Sin embargo, al producirse en la web, las consecuencias se potencian y expanden. Es importante saber los efectos que el cyberbullying trae aparejado para entender la importancia de prevenirlo y educar a partir de sus particularidades.

Para la víctima

La expansión y viralización del contenido logra que el dato o información difamatoria llegue a más personas que las estipuladas y que, por ende, se potencie la humillación. La falta de olvido en la web hace que el acto discriminatorio perdure en el tiempo.

Para el victimario

Las características de Internet hacen que el accionar del victimario quede registrado y que el hecho se asocie con su perfil, tanto en el presente como en el futuro.

Para todos los perfiles

La humillaciones producidas en persona responden a un contexto específico, tanto de la vida del agresor como de los cómplices y del agredido. En Internet, y gracias al no olvido de las publicaciones, este recor-

(4) Instituto Nacional de Tecnologías de la Comunicación de España, *Guía de Actuación contra el ciberacoso: padres y educadores*, [en línea] http://menores.osi.es/sites/default/files/Guia_lucha_ciberacoso_menores_osi.pdf, octubre 2012.

te temporal se pierde y la información perdura más allá de los contextos de los protagonistas. Esta característica hace que las consecuencias se extiendan y generen una constante relación entre ese hecho y los participantes, más allá de que estos se hayan arrepentido (en el caso del agresor o cómplice) o de que hayan podido superar lo ocurrido (en el caso de la víctima). Este es un punto central en el ámbito infantil, sobre el que el adulto debe actuar. Ya sea si se trata de un niño agresor o de un agredido, es necesario recordar que, al producirse en Internet, el acoso se vuelve un sello que perdurará en la reputación *online* del niño en el presente y en el futuro. Es fundamental trabajar el tema a partir de situaciones concretas, como una futura búsqueda laboral donde la agresión puede volverse un antecedente que un posible jefe probablemente tendrá en cuenta. Este tipo de ejemplo puede ser útil para evitar la participación en las discriminaciones web.

Dónde consultar

El Programa Nacional **"Con Vos en la Web"** tiene un espacio de consultas. Para utilizarlo hay que ingresar a www.convosenlaweb.gob.ar, y luego al link "S.O.S en la Web".

Por su parte, el Inadi, a través de su "Plataforma por una Internet Libre de Discriminación en Internet", ofrece asesoramiento y un sitio web donde denunciar los casos de acoso u hostigamiento: **www.inadi.gob.ar**

Cómo detectar casos de cyberbullying

Los niños o niñas víctimas de discriminación en Internet suelen manifestar cambios en su conducta, principalmente tristeza. Es probable que sufran variaciones en su rendimiento escolar y que estén pendientes de lo que ocurre en la web para controlar las publicaciones que otros hacen sobre ellos. Encerrarse y buscar estar solos también pueden ser síntomas a tener en cuenta.

Los adultos deben estar atentos a los cambios que se producen en el ánimo o conducta de los más chicos, para poder ayudarlos y acompañarlos.

Prevención y acción

- Proponer espacios de diálogo: la charla abierta con niños y niñas donde se les permita expresar lo que les ocurre, es indispensable para detectar en forma temprana los casos de ciberacoso.
- No minimizar ni exagerar la situación, aceptando lo ocurrido desde el acompañamiento.
- Evitar echarle la culpa a Internet ya que los comportamientos *online* condicen con los *offline* y, por ende, la web es solo un medio para llevarlos a cabo.
- No actuar sin escuchar las necesidades del niño. Una respuesta que no tenga en cuenta lo que el chico necesita puede exponerlo aún más y potenciar su humillación. Es por eso que, si bien es indispensable que el adulto acompañe, debe consensuar reglas de acompañamiento con el niño.
- Alentar al niño a que hable sobre el tema con amigos o personas cercanas. Mantener la situación en secreto potencia tanto su aislamiento como las consecuencias de la agresión.
- Desalentar actitudes revanchistas o vengativas, ya que solo conducen a mayor violencia y no conllevan soluciones.
- No responder a la discriminación con más discriminación. Incentivar al niño a que evite sumarse a discriminaciones hechas por terceros y reenviar mensajes ofensivos.
- Participar en las redes sociales. Ser parte en la educación sobre buenas prácticas en Internet, enseñándoles a establecer perfiles privados y a elegir como amigos solo a personas que realmente conozcan.
- Acudir al servidor o sitio web donde se establece el acoso. Denunciar, bloquear o eliminar a los acosadores.

Grooming

Información y consejos para entender y prevenir el acoso a través de Internet

¿Qué es?

Se llama grooming a la acción deliberada de un adulto de acosar sexualmente a un niño o niña mediante el uso de Internet. Quien ejerce el grooming, siempre es un adulto.

Estos adultos suelen generar un perfil falso en una red social, sala de chat, foro u otro: se hacen pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña que quieren acosar.

El mecanismo del grooming suele incluir un pedido de foto o video de índole sexual o erótica. Cuando el adulto consigue la foto o el video del niño o niña, comienza un período de chantaje en el que se amenaza a la víctima con hacer público ese material si no le entrega nuevos videos o fotos, o si no accede a un encuentro personal.

Tipos de grooming

Debemos distringuir entre dos tipos de grooming:

No existe la fase previa de relación. El acosador logra tener fotos o videos sexuales de los chicos mediante la obtención de contraseñas o el hackeo de cuentas. Con el material sexual o erótico en mano, extorsiona al chico o chica con mostrarlo si este no le entrega más o accede a un encuentro personal. En este caso, el material es obtenido a la fuerza.

Existe la fase previa de relación en la que el acosador generó confianza. En este caso, el material es entregado por el chico y la confianza se vuelve el instrumento indispensable. Para generar esa confianza, el adulto se vale de distintas herramientas:

- Se hace pasar por un chico o una chica menor, manipulando o falsificando fotos o videos.

- Toma los gustos y preferencias que los chicos vuelcan en la web para producir una falsa sensación de familiaridad o amistad. Aprovecha esa información para que los chicos piensen que comparten preferencias y, de esa forma, acelerar y afianzar la confianza.
- Utiliza el tiempo para fortalecer e intensificar el vínculo. El tiempo transcurrido varía según los casos: el abusador puede lograr su objetivo en una charla o esperar meses e, incluso, años. Esto ayuda a que el chico se olvide o deje de tener presente que, del otro lado, hay un desconocido y termine considerándolo un amigo.

El propósito en estos casos es que el chico o chica le muestre algún contenido sexual (foto o video, generalmente) a su "amigo" (el falso perfil de chat con quien ya se siente en confianza). Una vez que el material llega al abusador, se genera una situación de chantaje donde suele quedar en evidencia la mentira sobre la identidad del adulto, quien le pide al chico más imágenes o incluso un encuentro personal a cambio de no mostrar el material. La posición de poder en la que se encuentra el abusador se refuerza por su adultez y por la vergüenza que siente el chico al enterarse de que se expuso ante alguien más grande que puede hacer público el material privado.

Es necesario destacar la importancia que tiene la cámara web, ya que, en muchos casos, se vuelve indispensable para que el chico se exhiba ante el adulto. Como explicábamos anteriormente, los abusadores se valen de programas que producen un falso video para aparentar ser un o una joven.

Componentes constantes en este tipo de casos

Relación: se busca ganar confianza. Para lograr el objetivo, se apunta a generar confesiones íntimas y privadas, lo que puede tomar más o menos tiempo.

Amistad: se refiere al contacto para conocer gustos, costumbres y rutinas de los chicos.

Componente sexual: el material entregado por el chico se vuelve, luego, objeto de chantaje.

¿Cómo prevenirlo?

Internet ofrece muchas oportunidades a chicos y a grandes. Una de ellas es la posibilidad de conocer gente y, a través de las personas, distintas culturas, formas de pensar, gustos y preferencias. Pero también puede ser una herramienta que brinde nuevas posibilidades para el desarrollo de delitos previamente existentes. En este sentido, el abuso o acoso sexual a niños, niñas y adolescentes y la pedofilia no deben explicarse solo teniendo en cuenta las facilidades que ofrece la web. Esta debe ser comprendida como un instrumento capaz de potenciar los distintos tipos de abuso que podemos encontrar en la vida *offline*.

La principal forma de prevención del grooming no es prohibir que los chicos hablen con desconocidos en las redes sociales, sino brindarles herramientas para que comprendan los riesgos que existen cuando comparten datos personales en la web.

Cuando los chicos están aún en la infancia, la posibilidad de hablar con desconocidos efectivamente debe estar regulada por los padres o familiares. El desarrollo cognitivo de los chicos menores de 12 años hace que sea conveniente recomendarles evitar su contacto con extraños. Aquí vale pensar en los consejos tradicionales que nos dieron nuestros padres, abuelos y tíos: "no hables con extraños".

La principal forma preventiva en estos casos es, entonces, que los chicos comprendan que, más allá de la confianza ganada y de la amistad que se haya generado, los desconocidos con los que chatean continúan siendo desconocidos. La identidad en Internet no es tan fácil de corroborar como en el contacto cara a cara. Los chicos, nativos digitales, muchas veces no distinguen la vida *online* de la vida *offline*: nacieron con un universo donde los amigos pueden ser tanto los del colegio o los del barrio, como los del chat, Facebook u otra red social.

Para los adolescentes, en cambio, recomendamos reforzar el diálogo y la confianza, e inculcarles una mirada crítica y reflexiva sobre sus actitudes en la web.

Para evitar que los chicos den material que luego pueda ser usado como extorsión, y para brindarles herramientas de navegación segura, es necesario puntualizar un poco más respecto a la prevención. A continuación detallamos algunos puntos que debemos trabajar con ellos:

¿Qué pueden hacer los niños y adolescentes?

No dar información o imágenes comprometedoras por chat. Esta recomendación no debe limitarse a los desconocidos, ya que las fotos rápidamente pueden cambiar de contexto y quedar expuestas en la web. Es importante reforzar la idea de que el material que circula en Internet es difícil de borrar. Si alguna imagen íntima comienza a circular, va a verse asociada en el presente y en el futuro con las búsquedas *online* de la persona que protagonice el video o foto.

No utilizar la cámara web cuando se chatea con desconocidos. Del otro lado, pueden estar grabando lo que los niños, niñas y adolescentes muestren, tenga o no contenido sexual. La imagen es un dato personal que requiere cuidado y protección. Mostrarse a través de una cámara web es una forma de entregar material a un desconocido que puede hacerla circular o utilizarla para futuras extorsiones.

Conocer las buenas prácticas respecto de las contraseñas. De ese modo, puede prevenirse el robo de imágenes. Recordemos que:

- Colocar contraseña en todos los dispositivos (teléfono celular, tableta, netbook, notebook o computadora de escritorio).
- Utilizar contraseñas seguras: lo recomendable es que combinen números y letras, y que sean fáciles de recordar, pero difíciles de robar. Hay que evitar datos predecibles como el nombre y la fecha de nacimiento; 12345; DNI o el nombre más 1234.
- No compartir la contraseña. A excepción de los niños, a quienes les recomendamos que compartan las contraseñas con sus papás, los adolescentes deben evitar compartirla, incluso con amigos.
- Evitar usar la misma contraseña para todas las cuentas, ya que si alguien accede a una, podrá ingresar a todos los espacios donde se la use.

¿Qué pueden hacer los padres?

Concientizar a los chicos acerca de los peligros del anonimato y falsa identidad en la web. Hay que explicarles lo fácil que es abrir un perfil con datos falso.

Tener presencia en la vida *online* de los chicos. La charla y el conocimiento sobre las páginas web, las redes sociales y las personas con las que interactúan son indispensable. Así como conocen las rutinas de la escuela, el club o la calle, es fundamental que sepan qué gustos y rutinas tienen en su vida *online*.

Conocer las características de las páginas que los jóvenes usan. Para esto es importante que indaguen en sus políticas de privacidad, reglas y sus particularidades.

Acompañar a los chicos. Si bien, muchas veces, los padres sienten que saben menos que sus hijos respecto del uso de las TIC, ello no debería impedir que los acompañen y cumplan así con su rol de padres. Para los chicos es clave que los adultos les expliquen tanto las diferencias entre el mundo *online* y *offline*, como aquellas existentes entre los amigos que conocen cara a cara y los que solo conocen a través de la web.

Confiar en sus hijos. Los padres deben recordar que acompañarlos y conocer sus rutinas *online* desde ningún punto de vista significa violar la intimidad de los chicos (ingresar a escondidas a sus cuentas o casillas de mail).

Fases del grooming

Contacto y acercamiento. Al entrar en contacto con el chico, el acosador se vale de herramientas para mentir sobre su edad: fotos o videos modificados por programas web. En esta etapa se busca generar confianza y empatía.

Componente sexual. El acosador consigue que el chico le envíe alguna fotografía o video con componentes sexuales o eróticos.

Ciberacoso. Si el menor no accede a sus pretensiones sexuales (más material, videos eróticos o encuentro personal), el ciberacosador lo amenaza con difundir el material de mayor carga sexual a través de Internet (plataformas de intercambio de videos, redes sociales, foros u otros) o con enviarlo a los contactos personales del menor.

¿Dónde encontrarnos?

Para más información, pueden ingresar a nuestro sitio web, **www.convosenlaweb.gob.ar**, donde encontrarán material, guías y una sección para consultas denominada **"S.O.S. en la Web"**. Asimismo, podrán ver videos tutoriales que, entre otros temas, explican paso a paso cómo configurar la seguridad de las computadoras.

También pueden buscarnos en **Facebook** y **Twitter**, donde compartimos contenidos y recibimos consultas privadas que respondemos de forma inmediata.

Distinguir entre niños y adolescentes. Seguramente, los más chicos pueden necesitar un mayor grado de presencia. En estos casos, ante las incertidumbres de qué es lo mejor para ellos y qué hacer, vale la pena comparar nuestras decisiones respecto a la web con otras tomadas en la vida cotidiana como padres. Por ejemplo: ¿a qué edad los chicos pueden volver solos del colegio? Para este tipo de preguntas no hay una única respuesta, sino que cada padre la decide de acuerdo a la madurez del chico y a la relación que tenga con él. En Internet ocurre lo mismo: el padre debe pensar para qué está listo su hijo o su hija. En cualquier caso, creemos que la participación debe ser desde la educación y la compañía.

Aprender a configurar y mantener la seguridad/privacidad del equipo informático. Ello puede ayudar a evitar el robo de información comprometedora. Después de aprender cómo hacerlo, es menester transmitir esa información a los niños.

¿Cómo detectarlo?

Para detectar si un chico o chica es víctima de grooming u otro hostigamiento o acoso, recomendamos prestar atención a sus cambios de conducta o humor. Si un chico presenta repentina tristeza, descenso en el rendimiento escolar o necesidad de soledad, debemos charlar en confianza para entender qué le ocurre. Debemos tener presente que podría estar siendo víctima de alguna de las situaciones nombradas.

¿Qué hacer si pasa?

En caso de sospechar de un posible caso de grooming, la primera medida que deberíamos tomar es charlar con la víctima, procurando no avergonzarla o culparla. Recordemos que es sobre la vergüenza del chico/a donde el abusador funda su poder. Por ende, como adultos debemos evitar afianzar esa vergüenza y permitirle al chico/a contar lo que le pasó con la mayor sinceridad y libertad posible. Debemos, asimismo, evitar tanto revictimizarlo —es decir, echarle la culpa de lo ocurrido—, como interrogarlo en diferentes ámbitos y obligarlo a contar muchas veces lo que ocurrió.

Es indispensable que el adulto acompañe desde el afecto y la protección al chico o chica víctima de grooming y que recuerde que, durante el tiempo en el que —seguramente, por vergüenza—, dudó en contarlo, estuvo viviendo la extorsión de un abusador adulto.

A continuación, detallamos opciones de acción que, como adultos, debemos seguir una vez que tomamos noción de un caso de grooming:

Denunciar el perfil del acosador. Una de las principales herramientas que brindan las redes sociales es la de denunciar perfiles. De esa forma se puede dejar un precedente y, si otros también lo denuncian, se podrá conseguir que den de baja la cuenta del abusador y, por lo tanto, se evitará que replique su abuso con otros chicos.

Analizar el tipo de delito que se cometió. No es lo mismo si hubo un encuentro personal o si el abuso no traspasó la web. Estos datos serán importantes en caso de hacer una denuncia policial.

Pensar en hacer la denuncia penal. La decisión de realizarla, deberá partir del chico o chica que sufrió el abuso y de su familia. En caso de querer hacerla, será necesario guardar todas las pruebas necesarias.

Guardar las pruebas del acoso. Para ello, será necesario no borrar conversaciones, fotografiar o capturar la pantalla y almacenar esta información en algún dispositivo.

Otra buena opción es descargar la fotografía que haya enviado el acosador ya que, de esa forma se podrán conseguir datos útiles para una futura investigación (marca, modelo y número de serie de la cámara, fecha y hora en la que se tomó la foto; saber si fue retocada; identificar el programa usado para hacerlo y detectar datos sobre la computadora donde se la cargó).

La importancia de la denuncia hay que enmarcarla no solo en el delito cometido, sino en la certeza de que los abusadores no suelen atacar a una sola víctima, sino que actúan sobre varios chicos. Denunciando y logrando que se lo investigue y penalice, se evitará que el abusador continué perjudicando a otros niños.

Limitar la capacidad de acción del acosador. Como es posible que este haya tenido acceso al equipo del chico o tenga sus claves personales, recomendamos:

- Revisar el dispositivo (computadora, tablet o teléfono celular) para evitar el malware y cambiar las claves de acceso.
- Revisar y reducir las listas de contactos de las redes sociales, como así también configurar la privacidad en cada una de estas.

Infojus

Guía de amenazas

Las diez amenazas más peligrosas de Internet

Botnet

Es una red o grupo de computadoras zombis (infectado con malware) que, controlados por el propietario de los bots (atacante), toman control de equipos y los convierten en zombis. Pueden propagar virus y generar spam.

Esta última es la práctica más habitual de un botnet (enviar spam a direcciones de correo electrónico para la descarga de ficheros que ocupan gran espacio y consumen gran ancho de banda).

Los consejos para prevenir la amenaza son:

- Mantener las actualizaciones.
- Disponer de un firewall y un antivirus.
- Instalar programas que solo provengan de fuentes fiables.
- Ocultar nuestra IP (navegar de forma anónima).

Gusano

Es un malware que tiene la propiedad de duplicarse a sí mismo. Utiliza las partes automáticas de un sistema operativo, las que generalmente son invisibles al usuario.

A diferencia de un virus, un gusano (o worm, en inglés) no precisa alterar los archivos de programas; reside en la memoria y, desde allí, se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea, simplemente, consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Los gusanos son capaces de trasladarse a través de redes de computadores con el fin de realizar una actividad concreta incorporada en su código. Aun-

que su objetivo no es, en principio, generar daños en la PC, pueden instalar un virus o instalar un programa que actúe en segundo plano sin conocimiento del usuario.

Los consejos para prevenir la amenaza son:

- No instalar un software que no proceda de una fuente fiable. Para la obtención de nuevas versiones y actualizaciones, utilizar solo los servicios de descarga del fabricante o de los sitios autorizados por él.
- Actualizar periódicamente el antivirus, el software de seguriad y los sistemas operativos.
- No abrir correos electrónicos de desconocidos. Podrían contener enlaces o archivos nocivos para la PC.

Keylogger

Es un tipo de software que registra las teclas que presionamos en el teclado, para posteriormente guardarlas en un archivo y/o enviarlas a través Internet.

Permite a quien utiliza esta herramienta tener acceso a información importante de otros usuarios (contraseñas, números tarjetas de crédito y cualquier otro tipo de información privada).

Aplicaciones que realizan keylogging pueden ser distribuidas a través de un troyano o ser parte de un virus o gusano informático.

Los consejos para prevenir la amenaza son:

- Instalar un programa anti-spyware. Los programas anti-spyware pueden detectar diversos keyloggers y limpiarlos.
- Habilitar un cortafuegos o firewall. Ello puede resguardar el sistema del usuario del ataque de keyloggers y prevenir la descarga de archivos sospechosos: troyanos, virus, y otros tipos de malware.
- Utilizar monitores de red (llamados también "cortafuegos inversos") para alertar al usuario cuando el keylogger use una conexión de red. Esto da al usuario la posibilidad de evitar que el keylogger envíe la información obtenida a terceros.
- Utilizar software anti-keylogging. El software para la detección de keyloggers está también disponible. Como graba una lista de todos los keyloggers conocidos, los usuarios pueden realizar una exploración periódica en la lista, y el programa busca los artículos de la lista que estén en el disco duro.

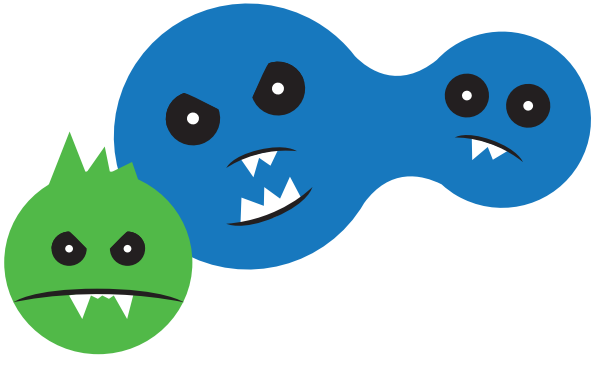
Pharming

Es el aprovechamiento de una vulnerabilidad en el software de los equipos de los usuarios que permite redirigir un nombre de dominio a otra máquina distinta haciendo creer al usuario que el sitio visitado es el original cuando, en realidad, es una copia del mismo.

De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de Internet a la página web que el atacante haya especificado para ese nombre de dominio.

Los consejos para prevenir la amenaza son:

- En caso de querer ingresar al sitio web de su banco, digitar la url en el navegador; evitar copiarla y pegarla de algún mail.
- Controlar los íconos de seguridad: suelen ser un candado en la barra del navegador o que la url comience con https. Algunos de los métodos tradicionales para combatirlo son la utilización de software especializado para la protección DNS (suele utilizarse en los servidores de grandes compañías para proteger a sus usuarios y empleados de posibles ataques de pharming y phishing) y el uso de complementos para los exploradores web, los que ofrecen protección a los usuarios domésticos.



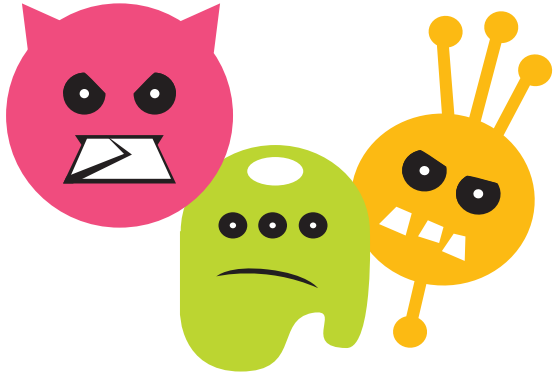
Phishing

Es un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas. Se comete mediante el uso de un tipo de ingeniería social que busca adquirir información confidencial de forma fraudulenta. Lo que se extrae puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica —por lo general, un correo electrónico o algún sistema de mensajería instantánea— e, incluso, por medio de llamadas telefónicas.

Los consejos para prevenir la amenaza son:

- No responder jamás a mails o mensajes de chats que nos soliciten información personal financiera o de cualquier otra índole. Las empresas y organizaciones que trabajan dentro del marco legal nunca solicitan datos personales, claves o números de cuenta de sus clientes o miembros a través de correos electrónicos o mensajes.
- No clickear en los enlaces que puedan aparecer en los referidos mensajes.
- Nunca acceder a páginas web comerciales, financieras o bancarias desde un enlace que venga en un correo electrónico. Si se conoce la dirección web, es preferible escribirla directamente en el navegador.
- No copiar y pegar la dirección de un sitio. Las redes de phishing operan generando sitios webs falsos, que poseen una apariencia similar a las páginas oficiales de las organización, precisamente para engañarnos.
- Verificar la legitimidad de un correo que solicite información confidencial, estableciendo contacto con la entidad antes de brindarla. Tal contacto debe llevarse a cabo a partir de información previamente conocida: apelando a números de teléfono o al personal de la organización.



Rootkit

Es un programa que permite un acceso de privilegio continuo a una computadora pero que, al corromper el funcionamiento normal del sistema operativo o de otras aplicaciones, mantiene su presencia activamente oculta al control de los administradores

Por lo general un atacante instala un rootkit en una PC después de haber obtenido un acceso al nivel raíz, ya sea por haberse aprovechado de una vulnerabilidad conocida o por haber obtenido una contraseña (por crackeo de la encriptación o por ingeniería social).

Ya instalado, el rootkit permite que el atacante oculte la siguiente intrusión y mantenga el acceso privilegiado a la computadora.

Pese a que los rootkits pueden servir para muchos fines, han ganado notoriedad a partir de su funcionamiento como malware, es decir, escondiendo programas que se apropian de los recursos de las computadoras o que roban contraseñas sin el conocimiento de los administradores y de los usuarios de los sistemas afectados.

Los consejos para prevenir la amenaza son:

- Prevenir que el atacante acceda a la PC. Para proteger a la computadora de accesos no autorizados, es necesario instalar un firewall que la proteja.
- Instalar una buena solución antimalware en la computadora y mantenerla permanentemente activa y actualizada.
- Mantener actualizadas las aplicaciones instaladas en la computadora. Verificar que los parches de seguridad sean los proporcionados por los fabricantes.

Sidejacking

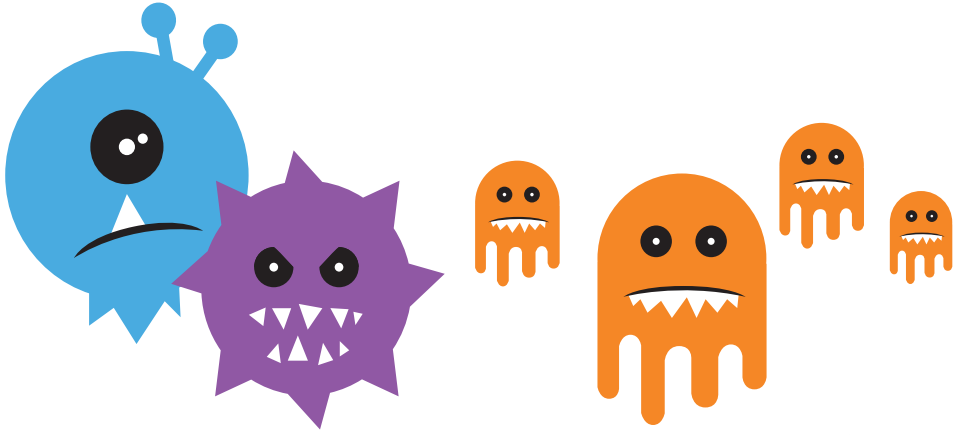
Es una técnica que consiste en copiar la información contenida en las cookies de una máquina conectada a una misma red (generalmente, en redes Wi-Fi públicas) para poder acceder a cuentas de la víctima y así robar su información.

Esta modalidad de ciberataque suele darse en aeropuertos, confiterías, bares, restaurants, etc., y en todo lugar público donde haya redes Wi-Fi y donde se comparta la misma red de conexión a Internet.

El atacante escanea y reemplaza las cookies de la víctima por sitio web, suplantando así la identidad. El usuario sigue usando su sesión sin darse cuenta de que otro usuario está también utilizándola.

Los consejos para prevenir la amenaza son:

- Evitar entrar a cualquiera de las cuentas de correo electrónico, sitios de compra *online*, redes sociales, a través de un navegador web en una red pública.
- Chequear que aparezcan https en la barra de direcciones. Al estar conectado y tener que ingresar datos personales a un sitio, es menester observar la barra del navegador para chequear que haya símbolos que denoten que la conexión es segura. Símbolos como, por ejemplo, un candado, seguido de las letras https (siglas de HyperText Transfer ProtocolSecure, Protocolo seguro de transferencia de datos) indican que no habrá fuga de datos cuando haya que utilizarlos.



Tabjacking

Es una amenaza que opera sobre las pestañas de los navegadores web. Espera a que pase un tiempo de inactividad sobre una pestaña que se queda abierta y la cambia por otra página falsa con la misma apariencia de la que se estaba utilizando.

Es decir, mientras el usuario está concentrado en otro sitio web, un código escrito en JavaScript detecta el intervalo y cambia el ícono y el contenido por uno de otro sitio, con la intención de robar información confidencial de los usuarios. El sitio original resulta reemplazado por otro que, aunque falso, se ve idéntico al anterior. La amenaza opera, incluso, sobre sitios populares como Facebook, Twitter, Gmail, etc. y otros de frecuente uso.

Los consejos para prevenir la amenaza son:

- No abrir mensajes sospechosos, con remitentes desconocidos, o servicios en los que no se esté dado de alta.
- Verificar la veracidad de los remitentes de cualquier tipo de mensaje, ya sea los recibidos por mail o red social, ya sea los provenientes de mensajes instantáneos. Preguntar a los amigos si realmente fueron ellos los que mandaron el link o llamar al banco para consultar sobre cualquier notificación de problema con la cuenta.
- Controlar que el software de seguridad sea actualizado periódicamente (firewall, antivirus, anti-spyware, etc.). Asimismo, asegurar el navegador con las últimas actualizaciones instaladas.

- En sitios web que requieran el ingreso de usuario y contraseña, siempre verificar que la dirección de la página sea auténtica. Los candados mostrados a la derecha de la barra de direcciones o en el borde inferior del navegador son una simple y práctica manera de realizar esa verificación.

Troyanos

Son amenazas que están diseñadas para permitir a un individuo el acceso remoto a un sistema. Una vez ejecutado el troyano, se puede acceder al sistema de forma remota y realizar diferentes acciones sin necesitar de permiso.

Se presenta como un programa aparentemente legítimo e inofensivo pero, al ejecutarlo, ocasiona daños severos.

Una de sus principales características es que no son visibles para el usuario. Un troyano puede estar ejecutándose en una computadora durante meses sin que este lo perciba.

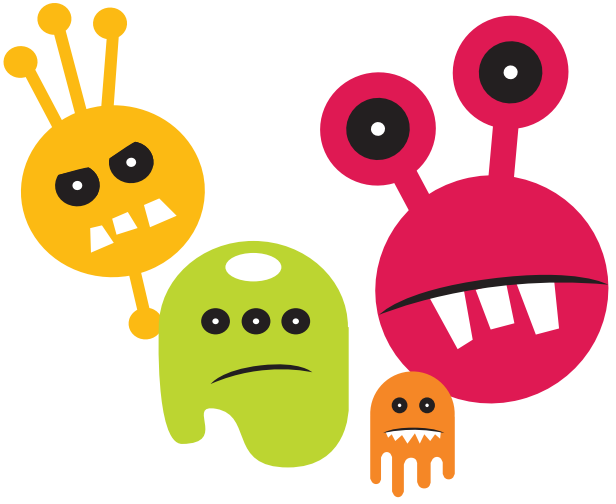
Algunas de las operaciones que se pueden llevar a cabo en la PC remota son:

- Utilizar la máquina como parte de una botnet (por ejemplo, para realizar ataques de denegación de servicio o envío de spam).
- Instalar otros programas (incluyendo malware - otros programas maliciosos).
- Robar información personal: datos bancarios, contraseñas, códigos de seguridad.
- Borrar, modificar o transferir archivos (descarga o subida).

La mayoría de infecciones con troyanos ocurren cuando se ejecuta un programa infectado con un troyano. Estos programas pueden ser de cualquier tipo, desde archivos ejecutables hasta presentaciones de fotos. Al ejecutar el programa, este se muestra y realiza las tareas de forma normal, pero en un segundo plano y al mismo tiempo se instala el troyano. El proceso de infección no es visible para el usuario ya que no se muestran ventanas ni alertas de ningún tipo.

Los consejos para prevenir la amenaza son:

- Disponer de un programa antivirus actualizado regularmente para estar protegido contra las últimas amenazas.
- Disponer de un firewall correctamente configurado (algunos antivirus lo traen integrado).
- Tener instalados los últimos parches y actualizaciones de seguridad del sistema operativo.
- Descargar los programas siempre de las páginas web oficiales o de páginas web de confianza.
- No abrir los datos adjuntos de un correo electrónico sin conocer el remitente.



Virus

Se presentan como programas aparentemente legítimos e inofensivos que, al ejecutarlos, ocasionan daños severos.

Los virus tienen por objeto alterar el normal funcionamiento de una computadora, sin el permiso o el conocimiento del usuario. Habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Así, pueden destruir, de manera intencionada, los datos almacenados en una computadora aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos.

Los virus tienen, básicamente, la función de propagarse a través de un software; no se replican a sí mismos porque no tienen esa facultad —como el gusano informático—; son muy nocivos y algunos contienen cargas dañinas (payloads) cuyos objetivos

son variados: desde hacer una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

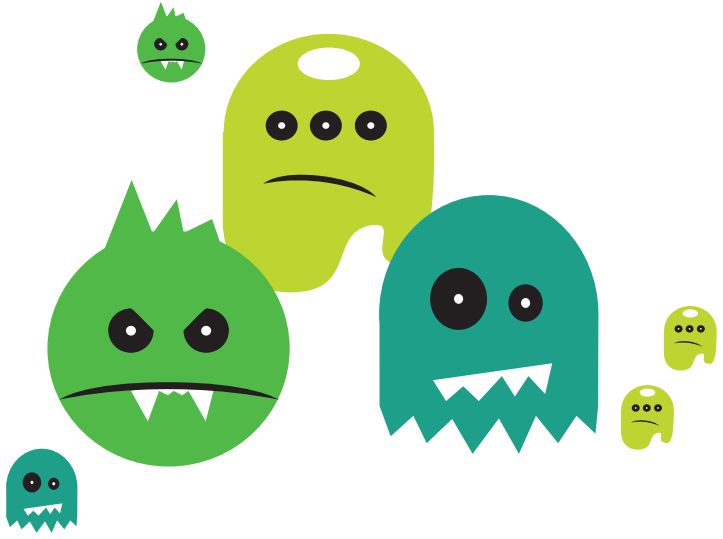
El funcionamiento de un virus informático es conceptualmente simple. Se ejecuta un programa que está infectado —en la mayoría de las ocasiones, por desconocimiento del usuario—. El código del virus queda residente (alojado) en la memoria RAM de la computadora, aun cuando el programa que lo contenía haya terminado de ejecutarse. El virus toma, entonces, el control de los servicios básicos del sistema operativo, infectando, de manera posterior, archivos ejecutables que sean llamados para su ejecución. Finalmente, el código del virus se añade al programa infectado y se graba en el disco, con lo cual el proceso de replicado se completa.

El nivel de peligrosidad de los virus se establece en función de los daños que son capaces de producir en el sistema —desde la aparición de mensajes hasta la total destrucción de la información de los equipos infectados—, y de su velocidad y facilidad de propagación. Su desarrollo y creación tienen mucho que ver con las vulnerabilidades existentes en el software de uso común, por lo que una primera barrera de prevención radica en mantener actualizado y al día nuestro sistema, además de utilizar herramientas de detección y desinfección.

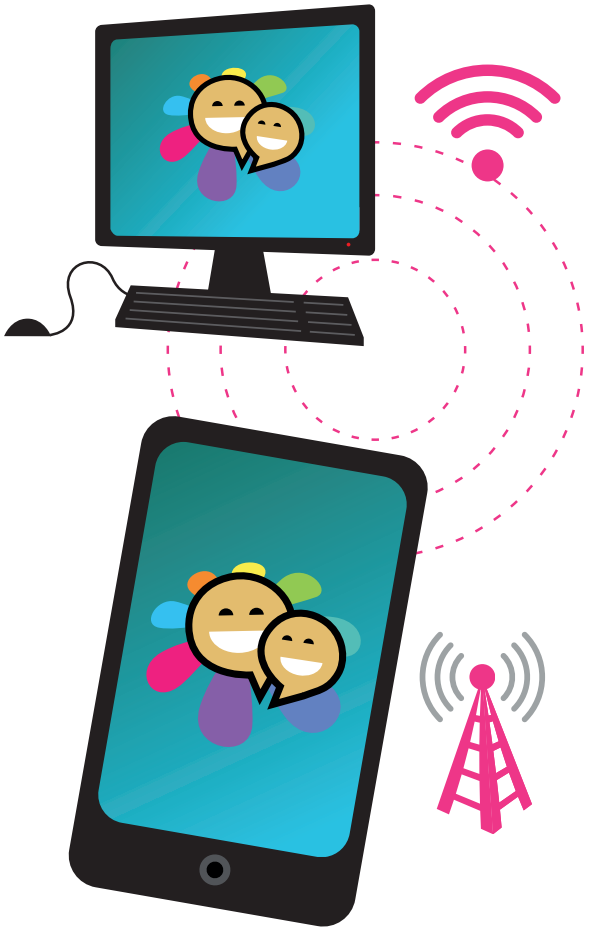
Por otro lado, en la actualidad existen numerosos servicios públicos donde podremos encontrar información sobre cualquier virus, además de información sobre cómo prevenir sus ataques.

Los consejos para prevenir la amenaza son:

- No ingresar el dispositivo de almacenamiento (pendrive, disco externo, etc) en computadoras que posean indicios de virus.
- No abrir correos electrónicos de desconocidos. Podrían contener enlaces o archivos nocivos para la PC.
- Tener actualizado el sistema operativo, el antivirus y el software de seguridad.



Redes inalámbricas



¿Qué es una red Wi-Fi?

Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Muchos son los dispositivos habilitados con Wi-Fi que pueden conectarse a través de un punto de acceso inalámbrico: computadoras personales, consolas de videojuegos, tablets, reproductores de audio digital, teléfonos inteligentes. Estos últimos, al compartir la conexión 3G, también tienen la posibilidad de ser utilizados como un router Wi-Fi.

¿Cuáles son sus ventajas?

Portabilidad

La comodidad que ofrecen las redes inalámbricas es muy superior a las redes cableadas porque cualquiera que tenga acceso a ellas puede conectarse desde distintos puntos, dentro de un rango. El alcance que este tipo de conexión tiene depende del equipo que se utilice.

Multidispositivo

Cualquier dispositivo que tenga la tecnología Wi-Fi puede conectarse a los puntos de acceso. Estos puntos pueden ser públicos o privados.

¿Cuáles son sus desventajas?

La gran desventaja que poseen las redes inalámbricas es la seguridad. Una red Wi-Fi sin protección puede ser usada por terceros para acceder a Internet —y, por lo tanto, a información privada o confidencial— o para cometer algún fraude, con las implicaciones legales que ello supone. Existen, además, algunos programas capaces de capturar datos de las redes Wi-Fi de modo invasivo, de forma tal que pueden calcular la contraseña de la red y, de esta forma, acceder a ella. En estos casos, no solo la conexión es más lenta sino que aquel que utiliza la red Wi-Fi tendrá acceso a la red interna y al equipo. Un hacker también tendría la posibilidad de interceptar nuestros datos y, de esta forma, obtener nuestras contraseñas de correo electrónico, leer conversaciones de chat, acceder a cuentas de crédito, etc.

¿Cómo proteger la red Wi-Fi?

Para asegurar la conexión, podemos implementar medidas de fácil aplicación para las que necesitamos solo conocimientos básicos y la ayuda de los manuales del dispositivo.

Es recomendable verificar bien las opciones de seguridad que brinda el router que estamos por instalar. Si utilizamos en forma correcta los medios de protección, tendremos una red Wi-Fi con un nivel de seguridad aceptable.

Modificación de los datos por defecto de acceso al router

Los routers y puntos de acceso vienen de fábrica con contraseñas por defecto; en muchos casos, públicamente conocidas. Para evitar que atacantes tomen el control desde el exterior y utilicen la banda ancha de nuestra conexión a Internet, es importante que cambiemos cuanto antes la contraseña por defecto del dispositivo.

Ocultamiento del nombre de la red

Para evitar que un usuario con malas intenciones pueda visualizar nuestra red, es necesario configurarla para que no se difunda su nombre públicamente. De esta manera, si alguien quiere conectarse a ella, solo podrá hacerlo si conoce el nombre de la red de antemano.

Para ocultar la red basta con limitar la difusión del nombre Service Set Identifier (SSID).

Uso de un protocolo de seguridad para proteger la red

Los sistemas más comunes para asegurar el acceso a la red Wi-Fi son el protocolo Wired Equivalent Privacy (WEP) , el protocolo WI-Fi Protected Access (WPA) y el protocolo WP2-PSK.

El protocolo WEP fue el primer estándar de seguridad para las redes inalámbricas y su protección es muy débil ya que, sin necesidad de ser un especialista, se puede romper la seguridad utilizando herramientas de hacking. En tanto, el WPA introdujo mejoras para superar las limitaciones que tenía el protocolo WEP.

El más seguro es el protocolo WPA, por lo que recomendamos su uso. También es posible utilizar el WPA2, que es la evolución del WPA. Es importante consultar la documentación del dispositivo antes de comprarlo y verificar que posea este nivel de seguridad.

Independientemente del protocolo que usemos, la forma de trabajo es similar. Si el punto de acceso o router tiene habilitado el cifrado, los dispositivos que traten de acceder a él tendrán que habilitarlo también. Cuando el punto de acceso detecte el intento de conexión, solicitará la contraseña que previamente habremos indicado para el cifrado.

En consecuencia, es necesario utilizar **siempre** un protocolo de seguridad y, en lo posible, el protocolo WPA o WPA2.

Consejos prácticos de seguridad

Generar contraseñas seguras

Es necesario que nuestras contraseñas sean seguras y cambiarlas cada cierto tiempo, lo que nos ayudará a lograr una mayor seguridad. Evitemos poner palabras obvias como "123456", "Qwerty", o alguna información personal como fechas de cumpleaños, aniversario, número de departamento, etc. Se recomienda combinar mayúsculas, minúsculas, números y símbolos para tener una contraseña más fuerte.

Apagar el router o punto de acceso cuando no se vaya a utilizar

De esta forma, reduciremos las probabilidades de éxito de un ataque contra la red inalámbrica y, por lo tanto, de su uso fraudulento.

En caso de tratarse de una cuenta con una red WI-FI de una casa u oficina particular, debemos recordar que, para impedir el acceso a cualquier persona, es necesario contar con una clave que solo el usuario conozca.

Riesgos de no tomar medidas de seguridad

El uso de nuestra red por parte de extraños puede implicar diversas consecuencias:

Económicas

Podría afectar el uso de banda ancha de la conexión.

Seguridad

Podría afectar los datos personales de nuestras respectivas computadoras.

Judiciales

Podría facilitar los medios para realizar diversos delitos *online*, como la pedofilia o la piratería informática.

Recomendaciones para el uso del celular como router WiFi

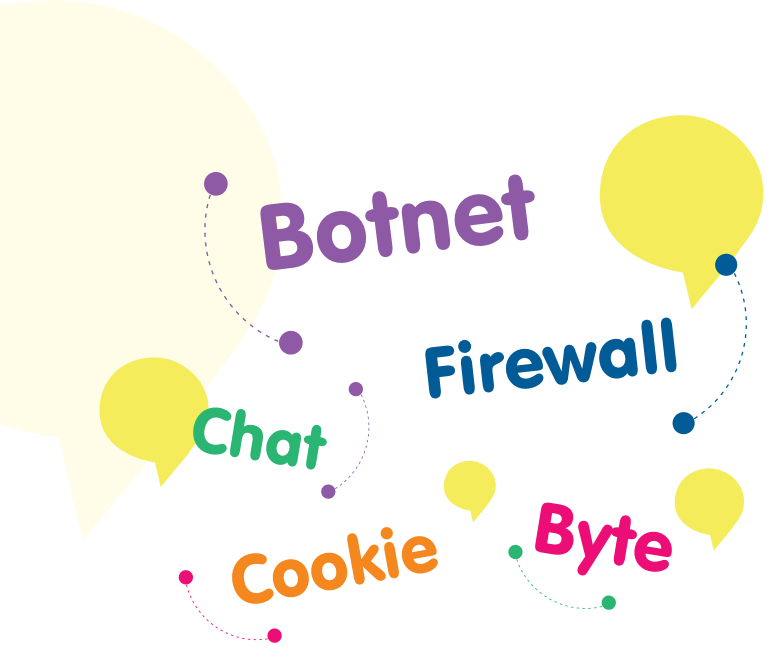
Al configurar un celular como un router Wi-Fi, es recomendable tomar las medidas antes mencionadas.

- Utilizar un tipo de protección WPA o WPA2-PSK (el tipo de modelo y marca determinará cuál podemos tener).
- Introducir una clave de acceso para mantener la privacidad de la red Wi-Fi portátil.
- Recordar que, si el dispositivo cuenta con un punto de acceso a Internet libre, cualquier desconocido puede utilizar la conexión 3G y, por ende, tener los mismos beneficios de cada uno de nosotros y correr los mismos riesgos.

Infojus

Glosario 2.0

Diccionario 2.0 para adultos: las palabras y definiciones más utilizadas en Internet



Adware: Tipo de programa que, en forma automática, muestra publicidad cuando el usuario lo usa o instala.

Antivirus: Aplicación que tiene por objeto la detección, bloqueo y eliminación de virus y otros códigos maliciosos.

Archivo, registro, base o banco de datos: Conjunto organizado de datos personales que ha sido objeto de tratamiento o procesamiento, electrónico o no —puede haber sido realizado en papel—, cualquiera que fuere la modalidad de su formación de almacenamiento, organización o acceso.

Bloqueo: Restricción total, parcial, temporal o permanente de un usuario dentro de un sistema informático (chat, foro, juegos *online*, etc). La principal causa de bloqueo es la violación a las normas de uso. El objetivo de esta acción es impedir que la persona bloqueada pueda contactarse y ver las publicaciones del bloqueador. El acto de bloquear es reversible, por lo cual puede realizarse en forma temporal.

Bluetooth: Especificación industrial que sirve para transmitir datos de manera inalámbrica y de uso extendido en dispositivos móviles (teléfonos, portátiles, tablets, etc.).

Botnet: Conjunto de computadoras (bots) infectadas por un virus o gusano que le permite al atacante realizar un monitoreo y control en forma remota.

Bullying: Nombre en inglés que recibe el acoso u hostigamiento escolar, que incluye maltrato tanto psicológico como físico. El bullying puede ocurrir en el aula como también en Internet, tomando en esos casos el nombre de ciberbullying.

Byte: Unidad que mide la cantidad de información, tamaño y capacidad de almacenamiento. Un *byte* equivale a 8 *bits*.

Cesión de datos: Toda revelación o comunicación de datos realizada a una persona distinta del titular.

Chat: Conversaciones escritas en Internet. A través de una conexión a la red, y a un programa especial o una web, es posible "conversar" (mediante texto escrito) en forma simultánea, con un conjunto ilimitado de personas.

Consentimiento del interesado: Toda manifestación de voluntad —libre, expresa e informada— mediante la cual el titular autorice el tratamiento de sus datos personales.

Ciberacoso: Situación en que un niño, niña o adolescente es atormentado/a, amenazado/a, acosado/a, humillado/a o avergonzado/a por un adulto por medio de Internet, teléfonos celulares, etc.

Ciberbullying: situación en la que un niño, niña o adolescente es atormentado/a, amenazado/a, acosado/a, humillado/a o avergonzado/a por otro niño, niña o adolescente por medio de Internet, teléfonos celulares, etc.

Cyberdating: Cita virtual, generalmente con un desconocido, a ciegas y acordada por algún medio tecnológico.

Código malicioso o malware: Programa capaz de realizar un proceso no autorizado sobre un sistema, con el propósito deliberado de generar perjuicios. Virus, troyanos, gusanos, son algunos ejemplos característicos de malware.

Compartir: Verbo que, en las redes sociales, se utiliza para hablar del acto de mostrarle a los contactos un contenido (posteo, video, foto, etc.) subido por otra persona.

Contraseña: Cadena de caracteres que identifican a un usuario. Se constituye a fin de permitir su acceso a un sistema o a recursos que son de uso restringido. Pueden utilizarse letras, números y símbolos, a fin de reducir su vulnerabilidad y garantizar una política de seguridad. En inglés se la conoce como *password*.

Cookie: Archivo de texto que emplean los servidores para identificar a los usuarios que se conectan a la red. Se almacena localmente en cada equipo y, cada vez que el usuario vuelve a visitar un sitio, es enviada nuevamente al servidor para que sea identificado. Posee también otras funciones como almacenar datos adicionales de quienes se conectan a un sitio, personalizar sus páginas, recopilar información necesaria para la navegación, etc.

Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Delito informático: Actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.

Etiquetar: Informar a los amigos que tienen cuenta en una red social de su aparición en algún posteo (foto, video o comentario). El acto de etiquetar se realiza colocando el nombre del contacto sobre el posteo generando un link directo con su cuenta personal en esa red social.

FAQ: Sigla que se refiere a la expresión inglesa *Frequently Asked Questions* —en español, Preguntas Frecuentemente Formuladas—. Documentos en línea que conforman un listado y dan respuesta a las preguntas más habituales sobre un tema o asunto particular. Son desarrolladas por quienes ya han detectado cuáles son las consultas o dudas más usuales de los usuarios de un sitio.

Firewall: Sistema de seguridad compuesto por programas y/o equipos en puntos clave de una red, para permitir solo el tráfico autorizado. Se lo emplea para restringir el acceso a una red interna desde Internet. Su objetivo es asegurar que todas las comunicaciones efectuadas entre la red e Internet se realicen conforme a las políticas de seguridad de la organización.

Freeware: Expresión que refiere a la expresión "de uso libre" y designa a aquellos programas que pueden ser empleados gratuitamente, creados sin fines de lucro.

Grooming: Acto deliberado de un adulto que contacta a un niño o una niña por Internet para establecer una relación de tipo sexual o erótica. En la mayoría de los casos, el mayor oculta o miente sobre su edad para generar mayor confianza con el niño. El grooming suele tener tres etapas: una primera, de conocimiento y amistad; una segunda, en la que el adulto le pide al niño alguna imagen (foto, video, etc.) con contenido sexual o erótico; y una tercera, de extorsión donde el acosador le exige más imágenes o, incluso, un encuentro personal a cambio de no exponer esa imagen íntima.

Grupo: Espacio similar a la página, al que se le agrega un foro o un ámbito de discusión sobre diferentes tópicos relacionados con el tema que los convoca.

Gusano: Programa semejante a un virus, que se diferencia de él por el modo en que produce las infecciones: los gusanos realizan copias de sí mismos, infectan otras computadoras y se propagan automáticamente en la red, independientemente de la acción humana. En inglés se los conoce como *worms*.

Geolocalización o georreferenciación: Aplicación que, desde cualquier dispositivo (teléfono celular, tablet, etc.) conectado a Internet, permite la obtención de información en tiempo real, así como la localización de la misma en el mapa con total precisión.

Hacker: Persona que tiene un profundo conocimiento sobre cómo funcionan y operan las redes, advierte errores y fallas de seguridad, y accede a los sistemas informáticos por diversas vías, generalmente con fines de protagonismo, aunque no necesariamente con malas intenciones.

Hardware: Todos los componentes físicos de la computadora, incluyendo también los periféricos.

Hoax: Mensaje de correo electrónico de contenido falso o engañoso, creado para que el destinatario lo reenvíe a todos sus contactos. Aparenta provenir de una fuente confiable y seria, y frecuentemente alerta sobre un virus. Propicia cadenas de solidaridad, difunde el otorgamiento de premios y regalos, etc.

Ingeniería social: Manipulación de las personas para que, voluntariamente, realicen actos que normalmente no harían. Generalmente, engañan a la gente para obtener información sensible como contraseñas, números de cuentas bancarias, tarjetas de créditos, etc.

Log-in: Sinónimo de lo que, en español, designa "iniciar sesión". Se utiliza para ingresar a una cuenta personal donde debe colocarse, por lo general, un usuario y una contraseña. Ejemplo de uso: "Me logueo a Facebook".

Log-out: Sinónimo de lo que, en español, designa "cerrar sesión". Se utiliza para salir en forma segura de una cuenta personal impidiendo que otras personas que utilicen el mismo dispositivo (celular, computadora, tableta, etc.) ingresen a esa cuenta. Una vez que se coloca "log-out" o "cerrar sesión", para volver a ingresar a la cuenta se deberá colocar nuevamente el usuario y la contraseña.

Mailbomb: Envío masivo de mensajes de correo electrónico excesivamente largos a la cuenta de correo de un usuario con el fin de saturar su capacidad de almacenaje o con intención de producir la caída del sistema.

Meme: Término que designa una idea o símbolo que se difunde rápidamente por Internet. Los memes más comunes en la web son los humorísticos, aunque también pueden tener un contenido serio, racista o discriminatorio.

Página: Espacios cuyo objetivo específico es reunir a personas que comparten los mismos intereses. En esos espacios los usuarios intercambian información relacionada con el tema que los convoca.

Perfil: Identidad que una persona tiene en las redes sociales (fecha de nacimiento, domicilio laboral, preferencias en cuestiones como música, libros, cine o moda, etc.). Los usuarios pueden compartir sus vínculos familiares, su número de teléfono u otros datos personales.

Perfil de usuario: Conjunto de datos, incluidos los de carácter personal, que los usuarios de redes sociales o sitios web colaborativos introducen en la plataforma al momento de su registro o al actualizarlo. Dicho perfil recoge información sobre sus gustos (cinematográficos, musicales, deportivos, etc.) y, en sus contenidos, el usuario puede incorporar en la red social fotografía, videos, textos, etc.

Pharming: Explotación de una vulnerabilidad en el software de los servidores DNS (*Domain Name System*), o en el de los equipos de los propios usuarios, que permite a un atacante redireccionar malintencionadamente al usuario a un sitio web falso o fraudulento, aunque de apariencia idéntica al verdadero. Se denomina también secuestro o envenenamiento del DNS.

Phishing: Delito basado en el uso de la ingeniería social para obtener información personal de los usuarios, especialmente sobre el acceso a servicios bancarios o financieros. Los estafadores que llevan a cabo este tipo de delitos suelen utilizar el correo basura (spam) como medio de propagación y contacto, engañando a los usuarios para que ellos aporten datos de carácter personal y privado.

Pic: Abreviatura de la palabra en inglés "picture", cuyo sinónimo en español es foto o imagen. Por lo tanto, cuando se habla de una Pic en la Web, se hace referencia a una foto o imagen.

Pirata informático: Persona que tiene como negocio la reproducción, apropiación o acaparación y distribución de distintos medios y contenidos como software, videojuegos, música o videos de los cuales no posee licencia o permiso del autor, con fines lucrativos, a través del uso de una computadora. Una de las prácticas más conocidas es la piratería de software. Erróneamente, se asocia a los piratas informáticos con los hackers.

Privacidad: Derecho de los individuos a controlar e incidir en la recopilación, almacenamiento y destino de sus propios datos personales.

Red: Grupo de computadoras o dispositivos informáticos conectados entre sí a través de cable, línea telefónica u ondas electromagnéticas (microondas, satélite, etc.), con el propósito de compartir recursos entre ellos y comunicarse. En tal sentido, Internet es una inmensa red a la que están conectadas otras subredes y se conectan millones de computadoras.

Red social: Sitio web que ofrece servicios y funcionalidades de comunicación para mantener contacto con otros usuarios de la misma red. Dentro de los servicios ofrecidos se encuentran: chat, foros, mensajería, blogs, etc. Cada usuario tiene un perfil configurado desde el cual comparte publicaciones y se comunica con otros usuarios.

Realidad aumentada: Nueva tecnología utilizada para aplicaciones móviles y tablets, que permite ver en la pantalla aquello que la cámara filma, agregándole una capa de datos. Así, por ejemplo, se puede filmar el obelisco y obtener datos sobre su construcción o ver cómo lucía una esquina determinada años atrás. También es posible mirar en tiempo real las casas de una cuadra en particular y ver superpuesto a la imagen qué casas están a la venta o alquiler y a qué precios sin que haya ningún cartel colocado.

Retweetear: Acto de compartir el tweet (posteo) de otro usuario de Twitter.

Seguir: Verbo utilizado en la red social Twitter para referir a la acción de seleccionar a un usuario para ver sus publicaciones en el sector de inicio. Los posteos (en este caso, llamado tweets) de los usuarios "seguidos" aparecen en forma instantánea en el inicio de nuestra cuenta.

Seguridad informática: Disciplina que incluye técnicas, aplicaciones y dispositivos para asegurar tanto la autenticidad, integridad y privacidad de la información contenida dentro de un sistema informático, como su transmisión.

Sesión: Duración del uso de un programa. Por ejemplo, cuando se inicia sesión en una red social, la persona se loguea (ingresa usuario y contraseña). La sesión finaliza cuando la persona se desloguea (cierra sesión).

Sexting: Envío de contenidos eróticos o pornográficos por medio de teléfonos celulares.

Software: Programa o aplicación programada para realizar tareas específicas.

Spam: Cualquier correo no deseado, que proviene de envíos automatizados y masivos. Afecta a correos electrónicos personales, foros, blogs y grupos de noticias.

Stalkear: Buscar información de una persona a través de la web, en general, y redes sociales, en particular.

Stalker: Persona que stalkea.

Spyware: Software espía. Aplicación informática que recoge información valiosa de una computadora, sin conocimiento ni consentimiento del usuario, vulnerando su privacidad. Puede capturar hábitos de navegación o mensajes de correo, ocasionar pérdidas económicas —resultado de recopilar tarjetas de crédito y claves de acceso—, y producir grandes en el funcionamiento de la computadora como bajo rendimiento, errores constantes o inestabilidad general.

Titular de los datos: Toda persona física o de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la ley 25.326.

Troyano: Programa que aparenta ser inofensivo y útil, pero que, una vez instalado, realiza acciones que afectan la confidencialidad y privacidad del usuario.

Tweet: Nombre del posteo en la red social Twitter

Tratamiento de datos: Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y, en general, el procesamiento de datos personales así como también, su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

URL: Sigla que refiere a *Uniform Resource Locutor* (en español, Localizador Unificado de Recursos). Dirección de acceso a páginas o archivos en Internet.

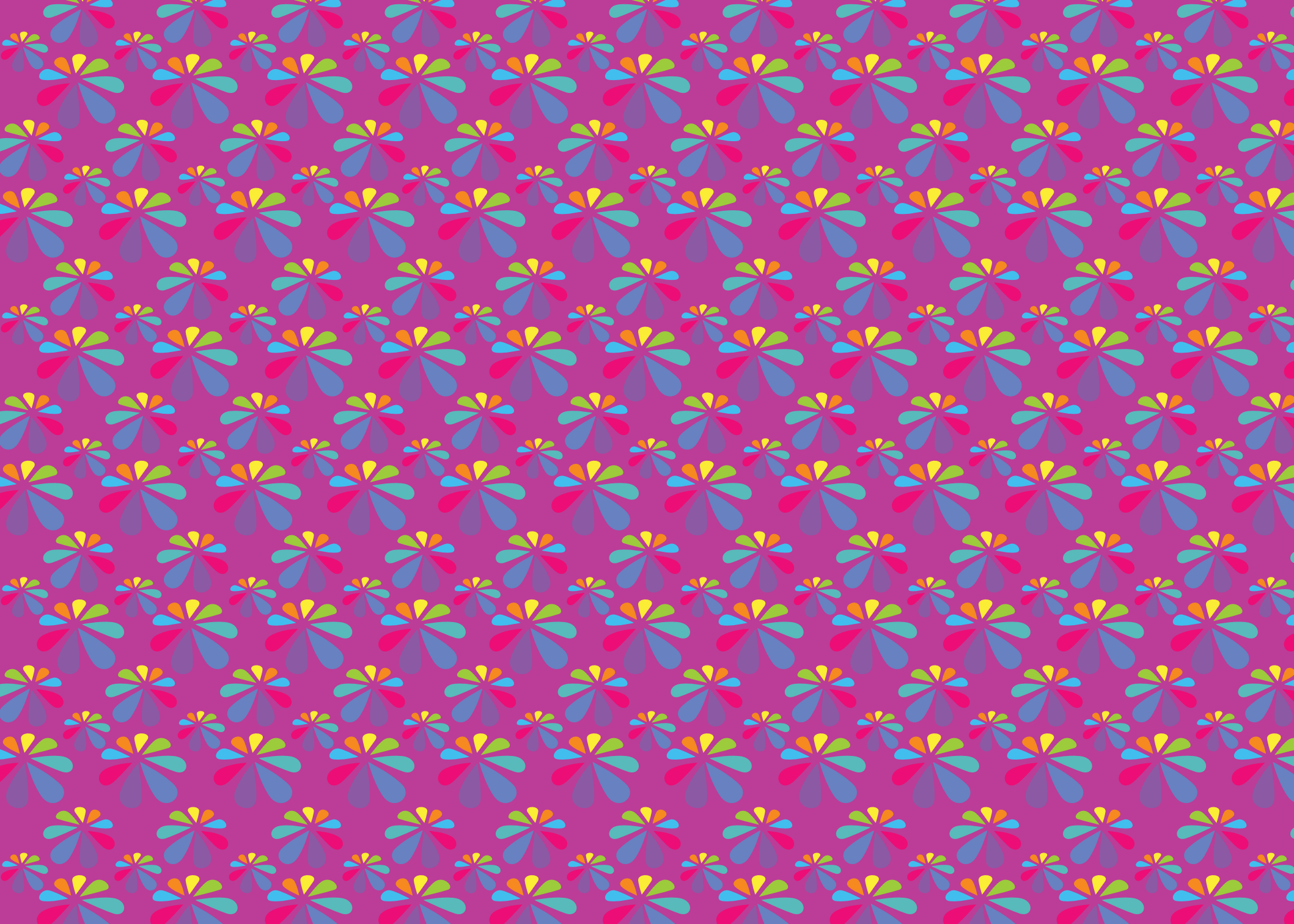
Virus: Programa diseñado para reproducirse y propagarse a sí mismo, sin conocimiento del usuario. Su función es la de infectar el sistema operativo y/o aplicaciones, y sus efectos pueden variar dependiendo de cada caso. Para que un virus se propague entre máquinas y sistemas, es necesaria la intervención humana a través de la descarga de archivos, el envío de adjuntos infectados por mail, el intercambio de discos USB, etc.

Web-Cam: Cámara de fotos y filmación que se instala o conecta con la computadora de escritorio/notebook/netbook/tableta. Su uso permite que las fotos o videos realizados puedan ser guardados o compartidos a través de la computadora y los programas que, desde ella, se usen (redes sociales, casilla de mail, etc.)

Wi-Fi: Abreviatura de *Wireless Fidelity*. Nombre comercial con el que se conocen los dispositivos que funcionan sobre la base del estándar 802.11, de transmisión inalámbrica.

Wiki: Web colaborativa instrumentada para el desarrollo de contenidos, uno de los logros más visibles de la Sociedad del Conocimiento.

Zombie: Computadora infectada por un troyano de acceso remoto, capaz de recibir órdenes externas y actuar en actividades maliciosas, sin conocimiento ni autorización del usuario.



PDP

con vos
en la web

Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación

Buscanos como ConVosenlaWeb en:

convosenlaweb.gob.ar | convosenlaweb@jus.gov.ar | (+5411) 4383-8512 Int.: 76712-09
Sarmiento 1118 5to. piso | C1041AAG | Ciudad Autónoma de Buenos Aires | Argentina