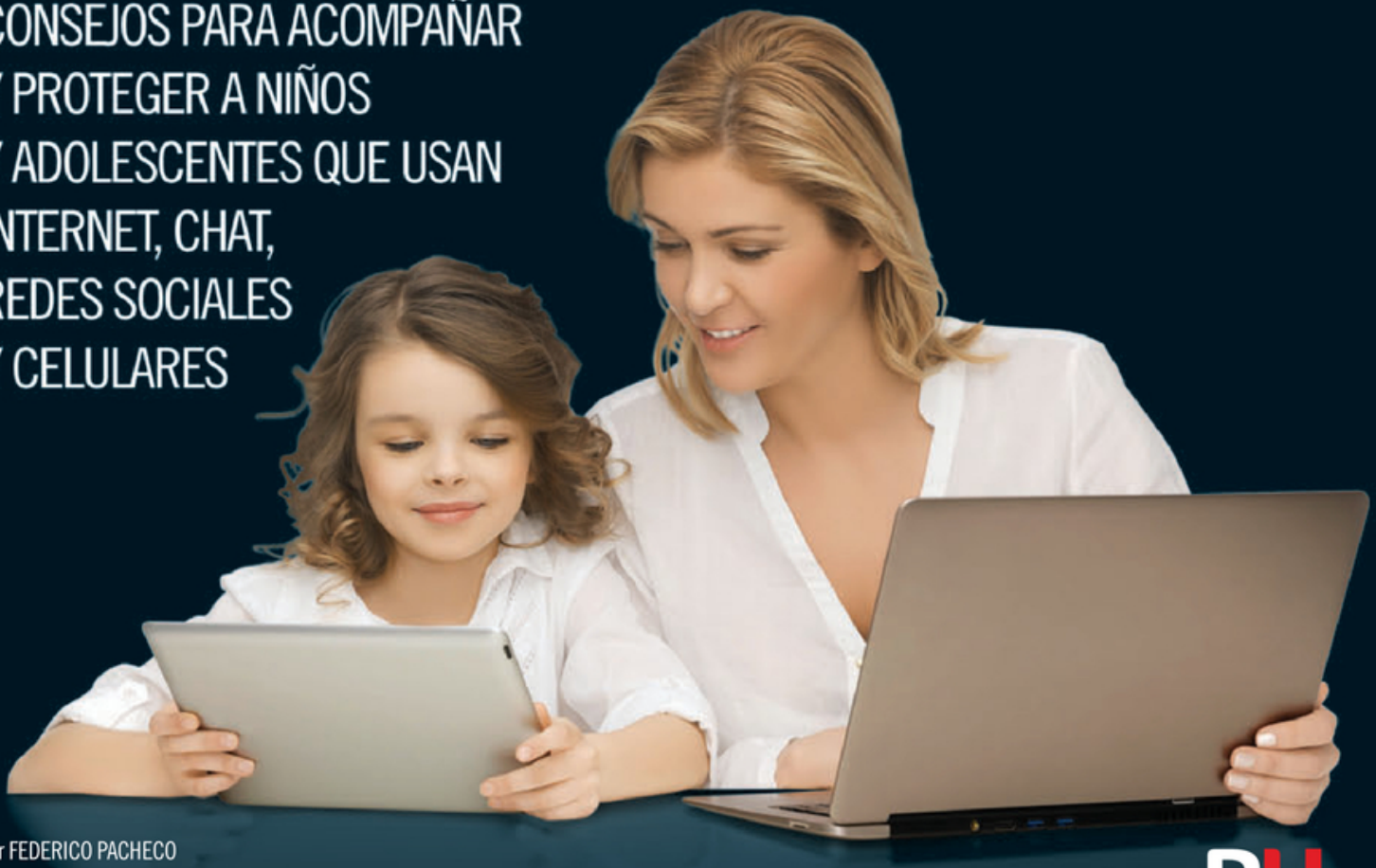
USERS

CÓMO COMBATIR EL GROOMING Y EL CIBERBULLYING

GUÍA PARA PADRES Y DOCENTES

LOS MENORES Y LOS RIESGOS DE LAS NUEVAS TECNOLOGÍAS

CONSEJOS PARA ACOMPAÑAR Y PROTEGER A NIÑOS Y ADOLESCENTES QUE USAN INTERNET, CHAT, REDES SOCIALES Y CELULARES



por FEDERICO PACHECO

PREVENCIÓN DEL CIBERACOSO Y OTRAS AMENAZAS ONLINE

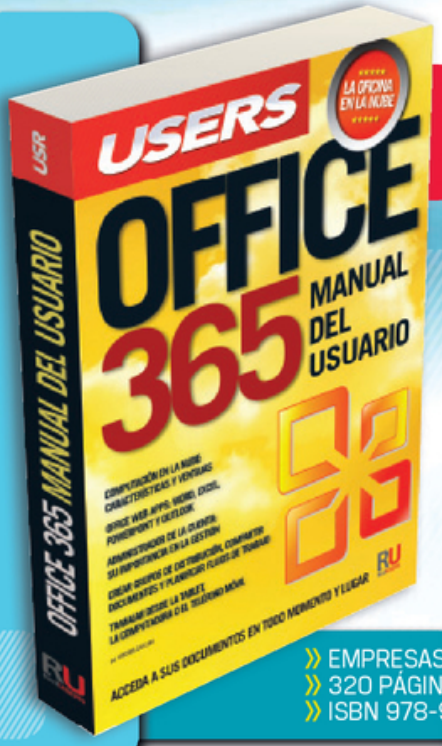
RU RedUSERS

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN



MÁS DE 150 ACTIVIDADES Y CONSEJOS PARA USAR LAS NUEVAS TECNOLOGÍAS.

» INTERNET / HOME
» 304 PÁGINAS
» ISBN 978-987-1857-61-6



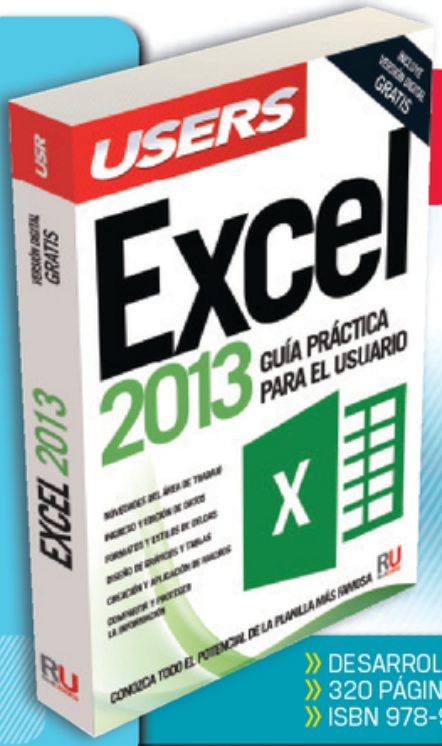
ACCEDA A SUS DOCUMENTOS EN TODO MOMENTO Y LUGAR.

» EMPRESAS / MICROSOFT
» 320 PÁGINAS
» ISBN 978-987-1857-65-4



USO DE INFORMÁTICA EN NIVEL INICIAL Y PRIMARIA

» HOME / INTERNET
» 320 PÁGINAS
» ISBN 978-987-1857-95-1



CONOZCA TODO EL POTENCIAL DE LA PLANILLA MÁS FAMOSA

» DESARROLLO / EXCEL
» 320 PÁGINAS
» ISBN 978-987-1949-08-3

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

MÁS INFORMACIÓN / CONTÁCTENOS

usershop.redusers.com +54 (011) 4110-8700 usershop@redusers.com

* SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // ** VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

LOS MENORES Y LOS RIESGOS DE LAS NUEVAS TECNOLOGÍAS

CONSEJOS PARA ACOMPAÑAR Y PROTEGER A NIÑOS Y ADOLESCENTES QUE USAN INTERNET, CHAT, REDES SOCIALES Y CELULARES

por Federico Pacheco

RedUSERS



TÍTULO: Los menores y los riesgos de las nuevas tecnologías
AUTOR: Federico Pacheco
COLECCIÓN: Colección Seriada
FORMATO: 24 x 17 cm
PÁGINAS: 192

Copyright © MMXIII. Es una publicación de Fox Andina en coedición con DÁLAGA S.A. Hecho el depósito que marca la ley 11723. Todos los derechos reservados. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Su infracción está penada por las leyes 11723 y 25446. La editorial no asume responsabilidad alguna por cualquier consecuencia derivada de la fabricación, funcionamiento y/o utilización de los servicios y productos que se describen y/o analizan. Todas las marcas mencionadas en este libro son propiedad exclusiva de sus respectivos dueños. Impreso en Argentina. Libro de edición argentina. Primera impresión realizada en Sevagraf, Costa Rica 5226, Grand Bourg, Malvinas Argentinas, Pcia. de Buenos Aires en VI, MMXIII.

ISBN 978-987-1949-11-3

Pacheco, Federico
Los menores y los riesgos de las nuevas tecnologías. - 1a ed. - Buenos Aires: Fox Andina; Dálaga, 2013.
192 p.; 24 x 17 cm. - (Seriada; 7)
ISBN 978-987-1949-11-3
1. Informática. I. Título
CDD 005.3



ANTES DE COMPRAR

EN NUESTRO SITIO PUEDE OBTENER, DE FORMA GRATUITA, UN CAPÍTULO DE CADA UNO DE LOS LIBROS EN VERSIÓN PDF Y PREVIEW DIGITAL. ADEMÁS, PODRÁ ACCEDER AL SUMARIO COMPLETO, LIBRO DE UN VISTAZO, IMÁGENES AMPLIADAS DE TAPA Y CONTRATAPA Y MATERIAL ADICIONAL.

RedUSERS
COMUNIDAD DE TECNOLOGIA

redusers.com

Nuestros libros incluyen guías visuales, explicaciones paso a paso, recuadros complementarios, ejercicios, glosarios, atajos de teclado y todos los elementos necesarios para asegurar un aprendizaje exitoso y estar conectado con el mundo de la tecnología.



LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

usershop.redusers.com // usershop@redusers.com

Federico Pacheco



Especialista en seguridad de la información, orientado a la consultoría, la investigación y la educación, ha prestado servicios tanto a empresas como a gobiernos. Cuenta con más de diez años de experiencia docente en distintos niveles de enseñanza, y forma parte de la cátedra de Seguridad Informática de la Universidad Tecnológica Nacional (UTN).

Participa periódicamente como expositor en conferencias locales e internacionales relacionadas con seguridad, tecnología, software libre y educación. En la actualidad, es director de membresías de ISSA Argentina y colaborador en varias ONGs. Ha publicado decenas de artículos en importantes revistas y sitios web especializados, y ha generado gran cantidad de material educativo para diferentes instituciones y para la comunidad en general.

Dedicatoria

A todos los niños que tuve la suerte de conocer.

Agradecimientos

A mis padres y maestros, quienes funcionando como ejemplo en algunos casos y como contraejemplo en otros me permitieron comprender que debía transitar el camino del educador.

Prólogo I

¡Extraños! ¡Peligro! Cuando era niña, me enseñaron a observar a mi alrededor. Si veía algo o a alguien desconocido, me movía con cuidado, solo para comprobar que todo estuviera "seguro". En nuestra vida online es muy difícil conocer o confiar en casi nada. Sin embargo, hay una luz. Organizaciones e individuos que concientizan y ofrecen educación al respecto. Los cinco principales temas para tener en cuenta al respecto son:

1) No sabemos qué no sabemos.
2) Nadie excepto uno mismo es responsable por sus comportamientos online.
3) Todo lo online puede ser "para siempre" e imposible de deshacer.
4) Las contraseñas fuertes y frases-contraseña son nuestras amigas.
5) Detenerse, pensar y conectarse. Algo muy simple que todos deberíamos implementar online.

Es un honor escribir estas palabras para mi amigo y colega Federico, una de esas personas que ayudan a otros a proteger su vida digital. ¡A disfrutar y aprender!

Liz Fraumann
Executive Director
Securing Our eCity Foundation
www.securingourecity.org

Prólogo II

A partir de la aparición de las nuevas tecnologías de la información, estamos asistiendo a una profunda transformación. La sociedad tecnológica forma ciudadanos, a quienes no les bastará estar alfabetizados en la cultura letrada, sino en un tipo particular: la de los textos electrónicos, las tecnologías digitales, los lenguajes audiovisuales y el manejo de información. Hoy, la sociedad nos presenta desafíos y, como consecuencia, nuestro compromiso es formar seres competentes con una dinámica de transformación constante, producto de avances científicos y técnicos.

Una nueva panorámica para el aprendizaje irrumpe y debe reconocer el campo de la experiencia en todo lugar y tiempo en que el individuo se desenvuelve. La educación ya no se circunscribe a la edad infantil ni a los formatos en los que las instituciones lo hicieron durante dos siglos. La educación sistematizada deberá reformular, modificar e instalar pedagogías relacionadas con la adquisición de estos nuevos alfabetismos y el acceso a conocimientos básicos que permitan conocer, comprender, interpretar y explicar los fenómenos y procesos del mundo natural, tecnológico y su relación entre ciencia y sociedad. En la medida que las tecnologías modifiquen nuestro entorno, será indispensable incorporar su manejo al aprendizaje continuo.

Los últimos diez años han sido testigos de una transformación tecnológica que trajo aparejada una nueva categoría de analfabetos. Con el surgimiento de esta sociedad, vertebrada en torno a las tecnologías digitales, aparecen nuevas formas de organización social, política y económica, nuevas maneras de comportarse y de relacionarse, trabajar, pensar y aprender. Una mayor cantidad de intercambios comunicacionales nos irrumpe y modifica no solo la producción y la circulación del saber sino los formatos en los que circula. Por ello, la mediamorfosis es la complementariedad de viejos y nuevos medios de comunicación que coevolucionan mediáticamente en la reconfiguración de usos y lenguajes. La mediamorfosis, teoría desarrollada por el canadiense Roger

Fidler, analiza la evolución tecnológica de los medios de comunicación como un todo y las relaciones entre las formas del pasado, del presente y las emergentes.

El autor nos invita a considerar la acción y la reflexión sobre los procesos tecnológicos, teniendo en cuenta el contexto actual, las generaciones, los peligros de Internet y otros temas que favorecen el desarrollo de valores, las capacidades creativas y la comunicación de los lenguajes digitales, verbales y no verbales. El planteo organizado, abierto y articulado a partir de situaciones reales admite diversos niveles de resolución y respuestas que favorecen la organización, la reflexión y la sistematización de los conocimientos propuestos, y posibilita el intercambio, potenciando la diversidad como ventaja pedagógica para repensar prácticas sociales.

Alicia Angela Iacovino
Fundación Solydeus

El libro de un vistazo

Este es un libro orientado a padres y docentes, en el que se explican los temas más importantes referidos al impacto de las nuevas tecnologías en relación con los menores. Analizaremos el contexto de Internet, los juegos de video, los celulares y otros aspectos que ningún padre o educador pueden dejar de conocer hoy en día.

*01 EL CONTEXTO ACTUAL

En este capítulo introduciremos el tema del contexto como factor relevante para comprender los conceptos subsiguientes. Veremos algunos aspectos en los que hemos tenido que evolucionar como sociedad para alcanzar la madurez tecnológica actual, y analizaremos cómo influyen los medios de comunicación e Internet en este proceso.

*02 DE LA GENERACIÓN X A LA GENERACIÓN Y

En este capítulo comenzaremos a hacer foco en los menores de edad, analizando para ello la transición entre las anteriores generaciones y la actual, así como también los paradigmas que han regido cada época. Además, introduciremos el concepto de brecha digital, uno de los aspectos más discutidos a nivel social con la llegada de las nuevas tecnologías.

*03 EL ESCENARIO VIRTUAL

En este capítulo nos centraremos en el análisis de distintas tecnologías que rigen el panorama actual de las comunicaciones, el entretenimiento y las relaciones sociales, entre las que hallaremos las redes sociales, la mensajería instantánea y los juegos de video. Asimismo, presentaremos la importancia de mantener sumo cuidado sobre la identidad digital y la virtual.

*04 LOS PELIGROS DE INTERNET

Este capítulo girará en torno al mundo de Internet y los riesgos que introduce, pasando por el tipo de contenidos y su legalidad, el software malicioso y los fraudes y engaños online. Además, veremos la importancia de crear conciencia para los casos de acoso virtual hacia los niños, ya sea por parte de pares o de adultos.

*05 EL HOGAR MODERNO

En este capítulo tomaremos la perspectiva de los padres para analizar los principales temas que deben tenerse en cuenta en relación con los menores de la familia. Tendremos en cuenta diferentes tecnologías de uso cotidiano, como teléfonos celulares, computadoras portátiles, tablet PCs, entre otras, y discutiremos aspectos que nos son técnicos y deben ser considerados por los padres en su relación con sus hijos respecto de las tecnologías.

*06 DESAFÍOS DEL EDUCADOR

En este capítulo nos enfocaremos en el punto de vista del docente que se relaciona con los niños en el contexto del aula. Analizaremos las tecnologías como parte activa del proceso educativo, la necesidad de su incorporación y las posibilidades con las que cuentan los educadores para alcanzar mejor sus objetivos.

*07 UN MARCO JURÍDICO ADECUADO

Este capítulo está enfocado en el marco legal de la tecnología, y responderemos a algunas de las preguntas más comunes relacionadas con su uso, los contenidos, la piratería y otras actividades online que suelen ser tema de discusión. Además, daremos un panorama del estado actual de la legislación en distintos países de Latinoamérica y el mundo.

*08 UNA VISIÓN DE FUTURO

En este capítulo haremos un análisis de la situación presente de cara a un futuro posible. El camino por recorrer será largo y lo iremos conociendo al caminarlo, ya que pocas cosas pueden ser predichas, aunque podemos prepararnos en muchos aspectos. Con esta necesidad de un enfoque integral presentaremos las conclusiones finales, dejando abierta la puerta al diálogo y el debate.

INFORMACIÓN COMPLEMENTARIA

A lo largo de este manual podrá encontrar una serie de recuadros que le brindarán información complementaria: curiosidades, trucos, ideas y consejos sobre los temas tratados. Para que pueda distinguirlos en forma más sencilla, cada recuadro está identificado con diferentes iconos:


CURIOSIDADES E IDEAS


ATENCIÓN


DATOS ÚTILES Y NOVEDADES


SITIOS WEB

Contenido

Sobre el autor 4
Prólogo I 5
Prólogo II 6
El libro de un vistazo 8
Introducción 12

*01 El contexto actual

La sociedad de consumo 14
De la información al conocimiento 16
Los medios de comunicación 18
Internet y la tecnología 21
La brecha digital 28
Resumen 29
Actividades 30

*02 De la Generación X a la Generación Y

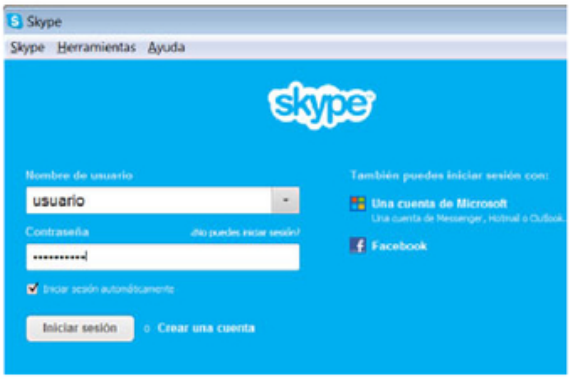
Un siglo de generaciones 32
Nativos digitales 37
Problemas de ayer y de hoy 39
Paradigmas obsoletos 42



El diálogo intergeneracional 44
Resumen 47
Actividades 48

*03 El escenario virtual

Vida online y lenguaje escrito 50
Redes sociales 53
Mensajería instantánea y chat 57
Juegos de consola y online 59
La identidad virtual 62
La nube y la información 65
Resumen 67
Actividades 68



*04 Los peligros de Internet

Contenido inapropiado 70
Descargas ilegales 73
Ciberbullying 78
Grooming 80
Usurpación de identidad 84
Malware 89
Phishing 95
Resumen 99
Actividades 100

*05
El hogar moderno

La familia y la tecnología 102
El protagonismo de la PC 105
Celulares y smartphones 108
Los límites posibles 112
Consejos para padres 114
Consejos para menores 119
Sobre el acoso online 121
Resumen 123
Actividades 124



*06
Desafíos del educador

Evolución y panorama de la educación 126
Información y contenidos 128
Tecnologías educativas 132
El nuevo rol del docente 135
Internet y tecnología en la escuela 139
Consejos para docentes 144
Resumen 147
Actividades 148



*07
Un marco jurídico adecuado

Tecnología y leyes 150
Nuevas necesidades 154
Legislación internacional 159
Leyes en Latinoamérica 164
Leyes en Argentina 166
Resumen aj171
Actividades 172



*08
Una visión de futuro

Tiempos de cambio 174
El camino por recorrer 178
Desafíos del mañana 181
Un enfoque integral 185
Resumen 187
Actividades 188

Introducción

Probablemente, recordemos los consejos que nuestros padres nos daban a medida que atravesábamos las etapas de crecimiento desde la infancia hasta la adolescencia. Frases como "cuidado al cruzar la calle", "no hables con extraños" o "no aceptes nada de desconocidos" formaban parte de las recomendaciones. Hoy en día, esos consejos y advertencias que nuestros padres nos dieron en base a su experiencia de vida ya no son suficientes, pese a que siguen siendo necesarios. Hoy los niños están expuestos a un mundo de estímulos nunca antes visto, a un exterior que ya no se representa solo de manera física en la calle o la escuela sino también de manera virtual, en un mundo hiperconectado que parece castigar el desconocimiento de sus reglas.

Frente a este nuevo escenario, donde las redes sociales conviven con los buscadores y los contenidos se mezclan con el entretenimiento, se hace necesario agregar nuevos conocimientos al manual invisible que un padre quisiera recibir cuando se enfrenta al desafío de criar a sus hijos. En el mismo maremágnum de información, una generación pareciera tender a naufragar en tanto que otra pareciera nadar alegremente sin una dimensión real de los peligros que acechan allí afuera. Es justamente de aquí que partimos para encarar este estudio.

La idea de este libro no es brindar una solución a todos los problemas relacionados con la tecnología y las diferencias generacionales sino más bien ofrecer un marco de referencia para la comprensión de los aspectos clave que requiere el planteo actual de un mundo que no cesa de generar conocimiento.

La mayoría de las experiencias presentadas en esta obra se derivan de incontables conferencias dictadas y conversaciones sostenidas con niños de todas las edades, apoyadas en las revisiones de psicólogos, pedagogos, educadores y otros profesionales que han contribuido a las conclusiones arribadas, además de la gran cantidad de conversaciones con padres y docentes inmersos de manera directa en la problemática.

Hoy sabemos que la principal clave para mejorar nuestra seguridad y la de nuestros hijos en estos tiempos yace, fundamentalmente, en la comprensión de las responsabilidades que conlleva el uso de la tecnología. De eso hablaremos en profundidad en este libro.

*01

El contexto actual

En este primer capítulo haremos un repaso de las condiciones y el contexto que nos han llevado a ver y definir el mundo actual tal como lo conocemos y lo experimentamos; y analizaremos el impacto del desarrollo tecnológico en la vida cotidiana. Además, veremos de qué manera influyen los medios de comunicación e Internet en ella.

- La sociedad de consumo 14
- De la información al conocimiento 16
- Los medios de comunicación 18
- Internet y la tecnología 21
- La brecha digital 28
- Resumen 29
- Actividades 30

La sociedad de consumo

A pesar de que a veces pareciera no haber ningún vínculo entre muchas de las tecnologías actuales y la evolución del siglo pasado, lo cierto es que el mundo fue dando pasos determinantes que en muchos casos se han superpuesto, integrando factores de distintas épocas en una síntesis que representa bastante objetivamente el camino andado.

Remontándonos algunas décadas atrás, encontramos uno de los más claros orígenes del solapamiento actual visible, cuando apareció lo que se conoce como la sociedad de consumo.

Cuando se habla de **sociedad de consumo** se está haciendo referencia al tipo de sociedad que, desde el punto de vista de la economía y la sociología, se encuentra en un estado avanzado de desarrollo industrial y capitalismo, caracterizada por el consumo de bienes y servicios de forma masiva, accesibles debido a su gran producción. Se la considera como un estado avanzado de la sociedad industrial, denominación que hace referencia a una antigua estructura social occidental donde se produjo la **revolución industrial** y que provenía de los cambios emanados desde la sociedad agraria. Lo ocurrido con posterioridad abarca en su conjunto el término **sociedad postindustrial**, y es allí donde aparece la sociedad de consumo.

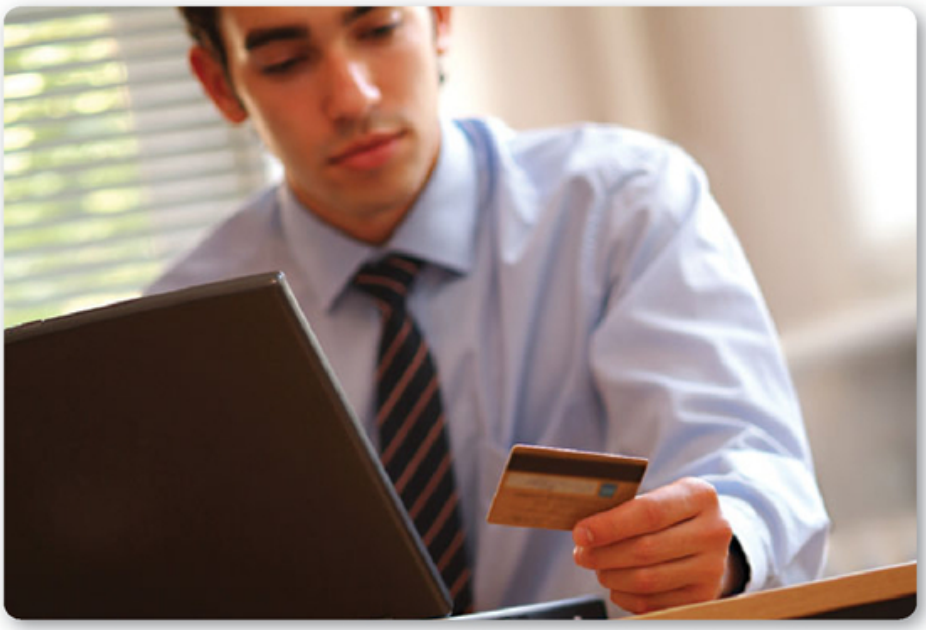


Figura 1. El comercio electrónico es el resultado de las facilidades que provee la tecnología a nuestra experiencia como consumidores.

Esta transformación hacia el consumo provino de ciertos avances de la técnica, en especial del inicio de la industria del **cine**, la invención del **automóvil** y la creación de la **radio**, que fueron acompañados por las ventas a crédito, la publicidad y la **obsolescencia planificada**. Todo esto permitió quebrar el aislamiento rural y conformar culturas en común, creando una especie de culto a las posesiones materiales.

Con el correr de los años, el acceso a la información, provisto y facilitado por las tecnologías (desde los avances en la industria editorial hasta los medios masivos de comunicación), fue generando una necesidad natural que permitió un viraje desde el consumo materialista puro hacia el **consumo de información**, presentada en libros, periódicos, radiodifusión y demás medios. Con esta nueva tendencia desembocamos en lo que conocemos como **sociedad de la información**.



Figura 2. **El condenado**, cuadro del pintor italiano **Lorenzo Paolini**, una metáfora del consumismo del siglo XX.

CARACTERÍSTICAS DE LA SOCIEDAD INDUSTRIAL

Esta sociedad buscaba la maximización de la producción mediante la organización del trabajo, facilitada por maquinaria que reemplazó a la mano de obra. Promovía la **producción en serie** y la especialización de las tareas, además del nuevo marco económico del mercado que regía las relaciones laborales.

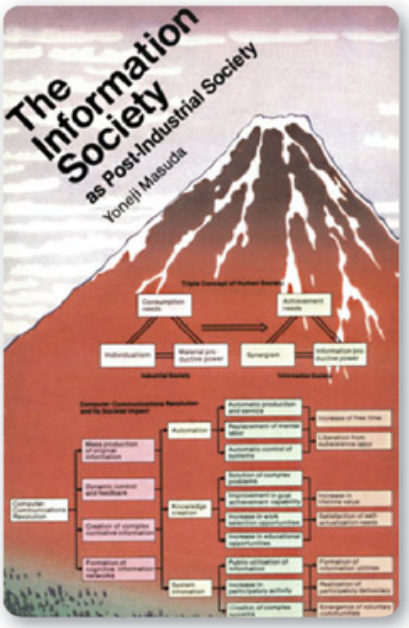
De la información al conocimiento

No podemos negar a esta altura que estamos atravesando una época de cambios, una época en la que terminamos por transformarnos en lo que se denomina **sociedad de la información**. Esta sociedad está representada por un conjunto de tecnologías que facilitan la creación, la modificación y la distribución de la información de forma tal que esta pasa a cumplir un rol fundamental en las relaciones socioculturales.



Figura 3. Además de acuñar el término **cibernética**, **Norbert Wiener** anunció la llegada de la sociedad de la información a mediados del siglo XX.

Esta conceptualización fue elaborada, entre otros, por el sociólogo japonés **Yoneji Masuda**, tal como lo manifiesta en su obra **The Information Society as Post-Industrial Society** (1981).



Si bien en un principio su connotación fue más bien política, ha querido describir el cambio en la relación con la información existente en el pasado y en la actualidad, pese a que en muchos aspectos solo haya llegado a ser una nueva utopía social.

Figura 4. En el libro **La sociedad de la información como sociedad post-industrial** se presenta el concepto de sociedad de la información.

Como sucesora de la sociedad de consumo, la sociedad de la información ha mediado entre aquella y una mucho más sofisticada, que es la **sociedad del conocimiento**. Esta fue mencionada por primera vez por **Peter Drucker**, ha estado emergiendo desde fines del siglo pasado y se refiere, en parte, al criticismo con el que las personas se relacionan con la información.

> LA SOCIEDAD DEL CONOCIMIENTO SURGIÓ GRACIAS AL USO MASIVO Y COTIDIANO DE TICS

Drucker afirmaba que lo más importante no era la cantidad de conocimiento generado sino la **productividad** que permitiría, y vaticinaba una sociedad en la que el principal recurso y **materia prima** sería el saber, donde la voluntad de generar más conocimiento mediante la aplicación del propio conocimiento debería estar sustentada en un esfuerzo inteligente de **organización** y **sistematización**.

Estas sociedades del conocimiento surgen de la **masificación** de las tecnologías de la información y comunicación (**TICs**) y de su uso en la vida cotidiana como parte de las **relaciones humanas** a partir de la potenciación de actividades que las personas ya realizaban hasta entonces pero sin contar con todas las herramientas actuales.

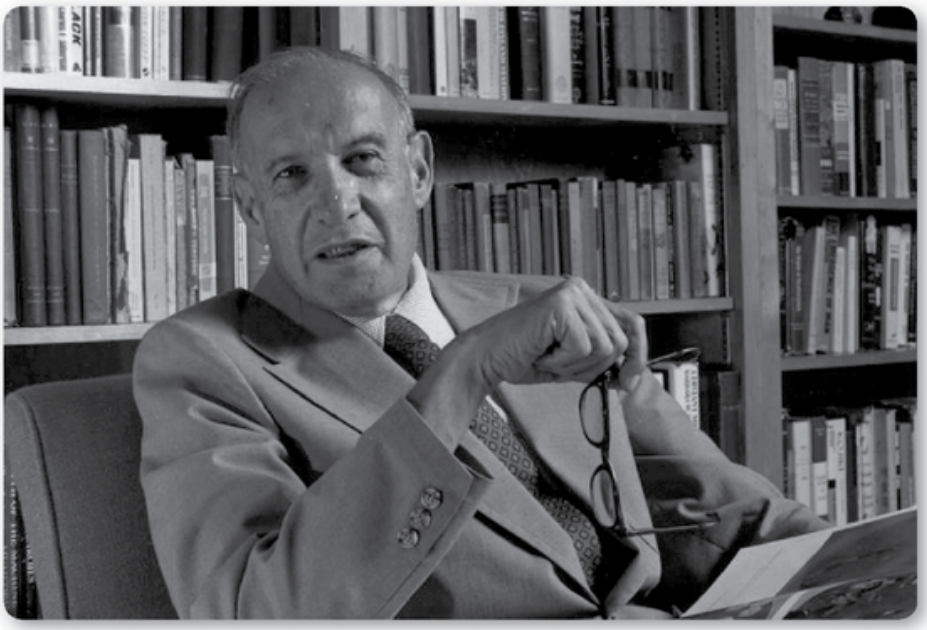


Figura 5. **Peter Drucker**, considerado el mayor filósofo del management del siglo XX, fue el primero en describir la sociedad del conocimiento.

Lo cierto es que, platónica o no, la idea de un mundo conformado por sociedades que tienen al conocimiento como **punto de referencia** podría ser un verdadero gran paso en la historia, si el **desarrollo tecnológico** se acompañara con una **justicia social** que garantice la **igualdad de oportunidades** para el acceso a la información que produce el conocimiento por medio del **esfuerzo individual**. Mientras el acceso a la educación continúe siendo un problema, como lo es hoy, el conocimiento estará siempre en manos de un sector y quienes provienen de familias menos beneficiadas, que por cuestiones económicas o geográficas no puedan contar con el acceso a las tecnologías que facilitan el acceso a la información, se seguirán reproduciendo sociedades en las mismas condiciones actuales: en completa **dependencia** de un golpe de suerte, una excepción a la regla, un estado benefactor, una iniciativa de caridad o un proyecto filantrópico.

Los medios de comunicación

Con el objetivo de **informar** y **entretener**, los medios de comunicación se han extendido desde la radio hasta los diarios y la televisión para llegar a grandes cantidades de personas en simultáneo. Por eso, en estos casos, hablamos más propiamente de ellos como **medios masivos** de comunicación (**mass media**). Estos medios son empresas privadas que poseen sus propios intereses económicos e ideológicos en función del grupo al que pertenezcan. Además, cuentan con una tendencia en sus contenidos con el fin de **influir** en su público mediante sus **mensajes** y sus **avisos publicitarios**. Como ciudadanos, estamos constantemente expuestos a los medios masivos

UN CAMBIO RADICAL

Según la **UNESCO**, el concepto de **sociedad del conocimiento** va aun más lejos que la **sociedad de la información**, porque apunta a transformaciones radicales y al desarrollo sustentable, y está sostenido principalmente en la libertad de expresión y el acceso a la información. La **Organización Mundial del Comercio** (**OMC**) asegura que las TICs motorizarán una **tercera revolución industrial**.

de comunicación, ya sea de manera directa por consumirlos nosotros mismos o por medio de la influencia en las personas que nos rodean, de manera que también influyen en nosotros de forma indirecta.



Figura 6. La **radio** surgió comercialmente en la década de **1920** y marcó un gran hito en el consumo de información.

Su concepción comenzó en la revolución industrial y ha crecido con el avance tecnológico, al punto de que los distintos medios han atravesado los mismos **ciclos**, comenzando por su **adopción como lujo**, pasando por su **masificación** y llegando a períodos de **crisis** por la introducción de otro medio. Podemos ejemplificar esto con los diarios y las revistas, la radio y la televisión, cada uno **superpuesto** al otro en su existencia, pero con fuertes cambios en algunos casos para poder **sobrevivir** al advenimiento de otro medio.

NOMBRES Y NÚMEROS

ICANN (Internet Corporation for Assigned Names and Numbers) fue creada en 1998 y es una organización internacional con sede central en California, Estados Unidos. Se encarga, entre otras cosas, de asignar direcciones de Internet a las distintas regiones del mundo y de manejar las políticas de los nombres de los dominios. Además, gestiona otras asignaciones numéricas y el sistema de resolución de nombres (**DNS**).

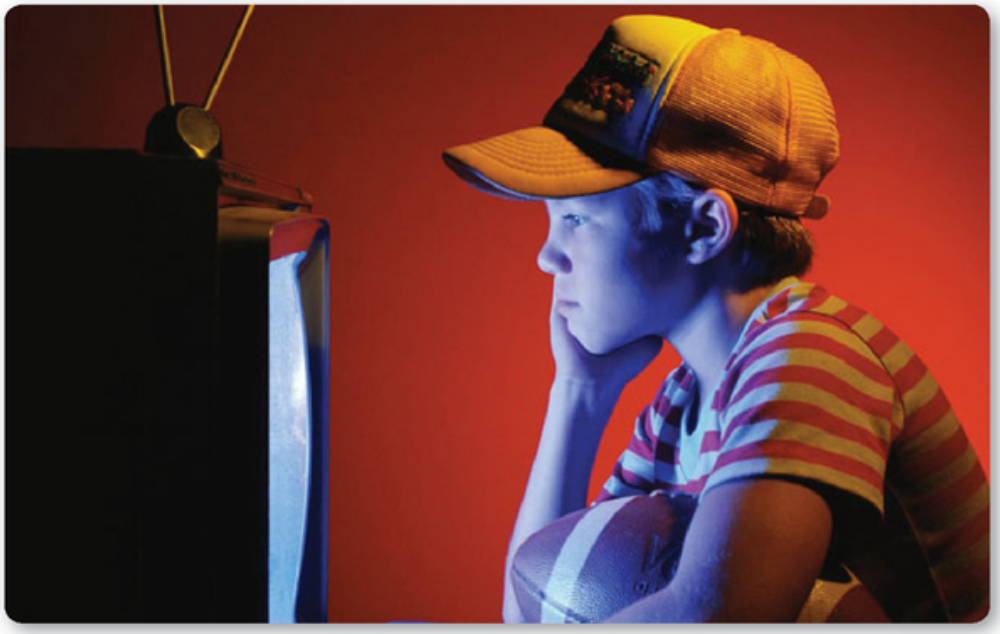


Figura 7. Históricamente, la televisión fue endiosada y demonizada por su impacto en la sociedad y su poder de influencia.

Se les atribuye a los medios masivos el haber ayudado al proceso de **globalización**, permitiendo la **interconexión** entre individuos y el **acceso** a la información. Además, cargan con la responsabilidad de haber limitado la **interacción personal directa** en favor de la individualización del consumo de la información.

Con su creciente poder, los medios han servido para las grandes **conquistas culturales modernas**, donde un mundo del norte se encontró con un mundo del sur y un hemisferio occidental se encontró con un hemisferio oriental. En esos encuentros, la fuerza de los más poderosos ha influido en las sociedades más débiles, que absorbieron muchas de sus costumbres y estilos, y asumieron muchos de sus criterios e ideas. La ausencia de toda coacción o



EL QUINTO PODER

En los últimos años surgió el movimiento denominado de **contrainformación**, que es la información generada por grupos o personas no vinculadas al poder político (en principio), de manera independiente. Ha tenido un auge exponencial con la llegada de las redes sociales y los teléfonos celulares, y ha de considerarse incluso como el quinto poder.

amenaza no deja entrever fácilmente los objetivos que el poder tiene detrás de estas acciones, por lo que resulta en una **aceptación natural** para las sociedades.



Figura 8. Con la globalización, llegó una nueva forma de comunicarse, viajar, estudiar y hacer negocios.

El impacto de los medios masivos es tan alto que se los ha llegado a denominar **el cuarto poder**, tras los tres poderes básicos de un Estado constitucional. Es esperable que exista entonces la intención de ejercer algún tipo de control sobre los medios –por lo que hay algunos temas que siempre están sobre la mesa, como la libertad de prensa, la censura y la **autorregulación**–, que depende de los distintos países y sus leyes.



Figura 9. El movimiento de **contrainformación** surgió de manera espontánea desde usuarios individuales que producen información independiente.

Internet y la tecnología

Hablamos de Internet como un grupo de redes interconectadas que funcionan de manera descentralizada y se comunican mediante la familia de **protocolos** de comunicación llamada **TCP/IP**. Sus

inicios datan del año 1969, al establecerse la primera interconexión de computadoras entre cuatro universidades estadounidenses en el contexto del proyecto **ARPANET**. Suele confundirse Internet con la **World Wide Web** (**WWW**), aunque esta última no es en sí una red sino un conjunto de protocolos que facilita el acceso a **documentos hipertextuales**, y que fue desarrollada en 1990 por **Tim Berners Lee** y su equipo de investigadores.

La confusión radica en que la **WWW** utiliza normalmente Internet como medio para su transmisión, y dado que las páginas que la gente consulta suelen estar encabezadas por la sigla **www**, no se ha tardado en pensar que "eso" era Internet. Además, el mismo equipo desarrolló el protocolo **HTTP**, que es el que se utiliza principalmente para acceder a los contenidos de la Web.



Figura 10. **Tim Berners Lee**, el padre de la **World Wide Web**, es el físico británico que creó los protocolos **HTML** y **HTTP**.

A medida que la información producida en la Web fue creciendo, encontrarla se hizo cada vez más dificultoso. Debido a eso, a principios de los años 90, comenzaron a surgir los **buscadores**, el primero de los cuales se llamaba **Wandex**, hoy inexistente. Después, aparecieron **Lycos**, **Altavista**, **Excite**, **Yahoo!** y otros, y recién en 1998 vio la luz el mayor de los gigantes, **Google**, que con el tiempo cambiaría para siempre la experiencia del usuario en Internet.

La **Internet World Stats** (**www.internetworldstats.com**) –una organización que se encarga de realizar estadísticas sobre el uso de Internet en el mundo– determinó que para mediados de 2012 la cantidad de usuarios en el mundo era de más de **2.400 millones**, lo que representa el **34% de la población mundial**. Por supuesto que la distribución de la conectividad es completamente desigual, existen **diferencias abismales** entre los países desarrollados y los del tercer mundo. Sin embargo, se pueden encontrar algunas paradojas, como, por ejemplo, el caso de la **Argentina** que, pese a sus características de subdesarrollo y constante crisis social y económica, cuenta con casi **70% de penetración**, por encima de gigantes industrializados como **Brasil** (45%) y **México** (37%), aunque por debajo de los **Estados Unidos**, con 78%.

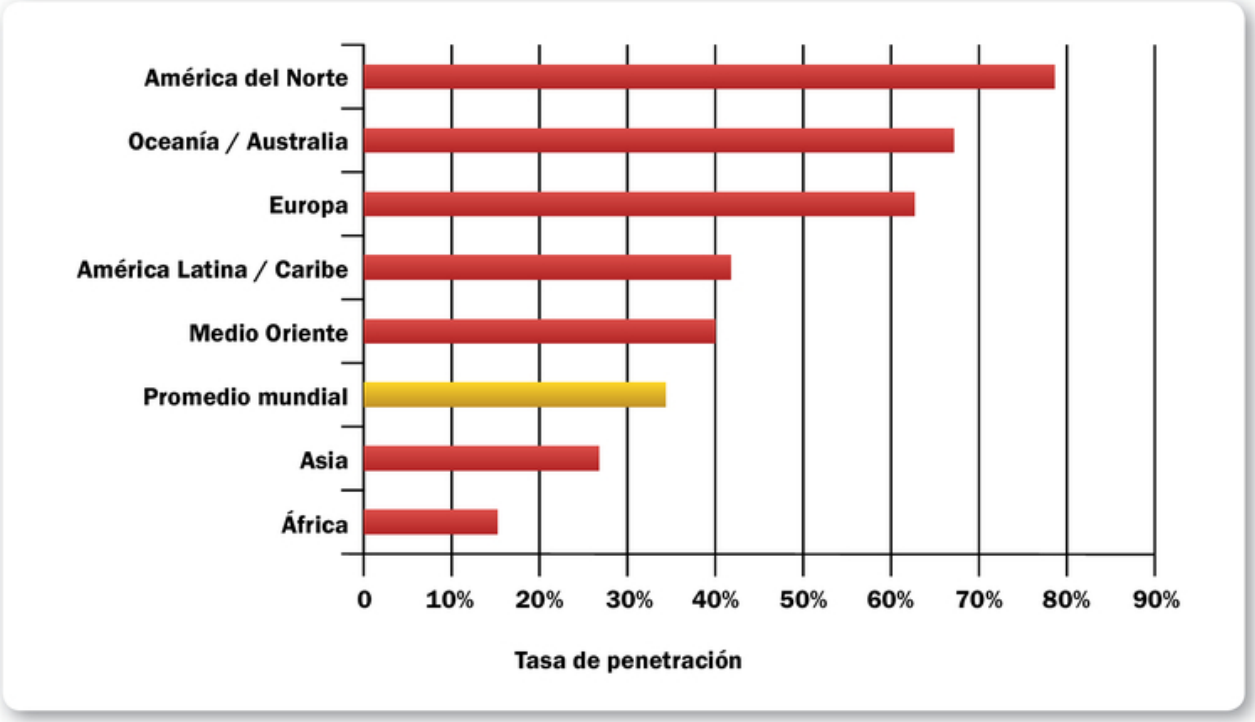


Figura 11. Penetración de Internet en las distintas regiones del mundo según las estadísticas de **`Internet World Stats`**.

Más allá de las estadísticas, es lógico y acertado pensar que los países del hemisferio norte son los **principales beneficiarios** y dueños de la infraestructura de Internet (el hardware, el software y los contenidos), en tanto que los del hemisferio sur, como en muchos otros aspectos, se encuentran a una gran distancia de aquellos.

Una conexión a Internet ofrece posibilidades de acceso a la información de manera casi instantánea, **comunicación** con otras personas, **entretenimiento** y **educación**; y su buen uso, apoyado en una concientización adecuada, puede hacer una gran diferencia en el resultado final del proceso educativo de los menores. Encontrarse con todo ese universo por descubrir motiva en los niños la **curiosidad natural** que los caracteriza; sin embargo, ese encuentro con un **mundo virtual** tan **desregulado** puede derivar en problemas que, aunque se espera tener bajo control en los años venideros, aún no han tenido solución aparente.

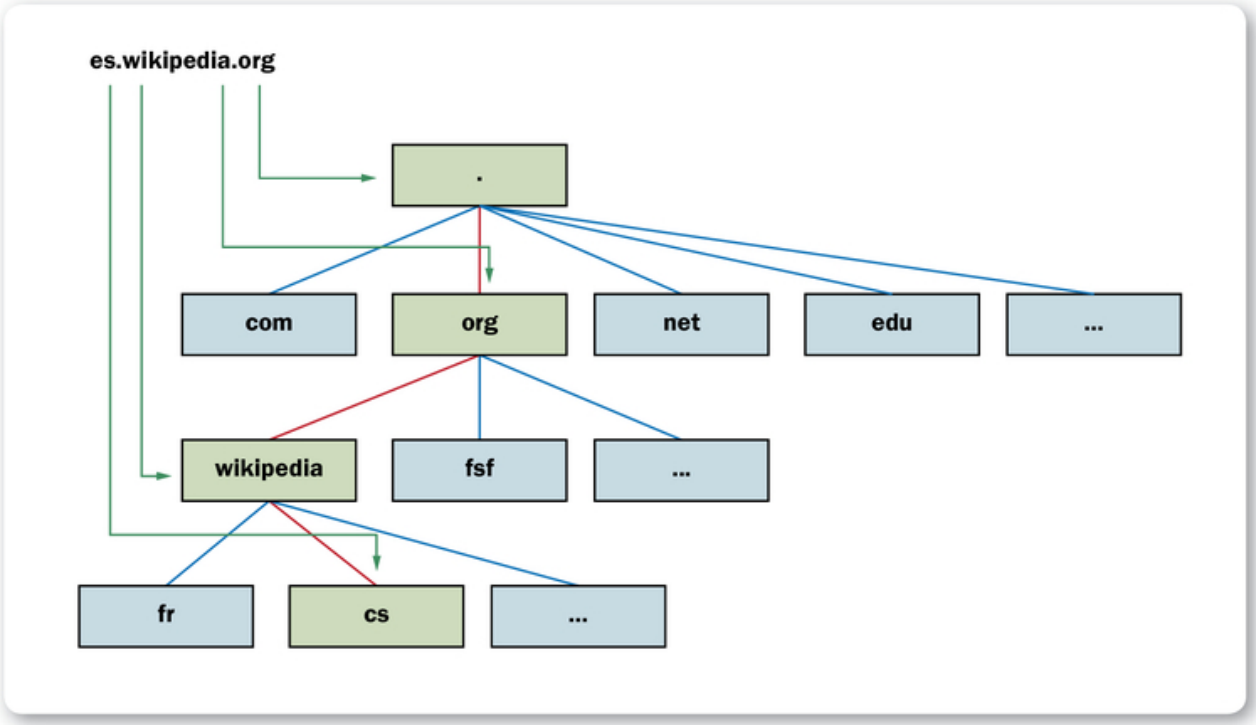


Figura 12. Los nombres de dominio en Internet tienen una jerarquía separada por puntos para poder ser referenciados.

DOMINIOS DE INTERNET

En Internet, se llama **dominio** al nombre asociado a un sistema conectado a la red. Este nombre permite referenciar los sitios y servicios con denominaciones que contengan una jerarquía identificable en función de distintos criterios, como el país de origen o el tipo de sitio (**.com**, **.br**, **.ar**, **.edu**, etcétera). Por medio de esta abstracción, un servicio de red logra la independencia geográfica y de su proveedor.

La gran posibilidad de acceso a la red global se vio acompañada de una serie de tecnologías que comenzaron a permitir la interacción con ese mundo sin la necesidad de contar de manera directa con una **PC**. Así, teléfonos celulares, **tablet PCs**, televisores y hasta electrodomésticos de uso cotidiano comenzaron a sumar funcionalidades que transformaron a Internet en algo que se puede encontrar potencialmente en todos lados, solo contando con algún dispositivo de acceso y una conexión.

Por su parte, las conexiones también evolucionaron desde los primeros **módems** de acceso telefónico (**Dial-Up**), que admitían velocidades menores a **56 Kb/s**, hasta las conexiones de **banda ancha**, que proveen hasta varios megabits por segundo de velocidad y **tarifa plana** que permite estar las 24 horas del día online.



Figura 13. Mapa de los cables submarinos que interconectan los principales nodos mundiales de Internet (Fuente: Telegeography).

LAS DIRECCIONES IP

Una dirección **IP** (Internet Protocol) es un conjunto de números que permite identificar de manera jerárquica un dispositivo de red que utilice el protocolo **TCP/IP**. Cada conexión a Internet cuenta con una dirección IP pública con la cual se identifica en la red, y las redes internas poseeen direcciones de IP privadas para identificarse entre sí pero sin validez en Internet.

Pero eso no es todo, ya que al poco tiempo aparecieron las conexiones inalámbricas **Wi-Fi** y **satelitales**, que extendieron la posibilidad de conexión sin cables de forma que hasta en un espacio público podemos acceder a la red.

Luego, fuimos testigos del nacimiento de las redes digitales de telefonía celular con capacidad de conexión a Internet por medio de tecnologías como **3G**, **EDGE** y otras.

Fue la telefonía celular, nacida comercialmente en 1983, la que empujó en gran parte el cambio de paradigma en materia de comunicaciones personales, independizando prácticamente al usuario de su lugar físico, que hasta ese entonces estaba limitado por las líneas de telefonía cableada en las ciudades.

El impacto de los teléfonos móviles en la sociedad actual es tal que, por su gran avance, se los ha denominado la **cuarta pantalla**, nombre que proviene de una extensión de las **tres pantallas** anteriores con las que se relacionan las personas: el **cine**, la **televisión** y la **computadora personal**.

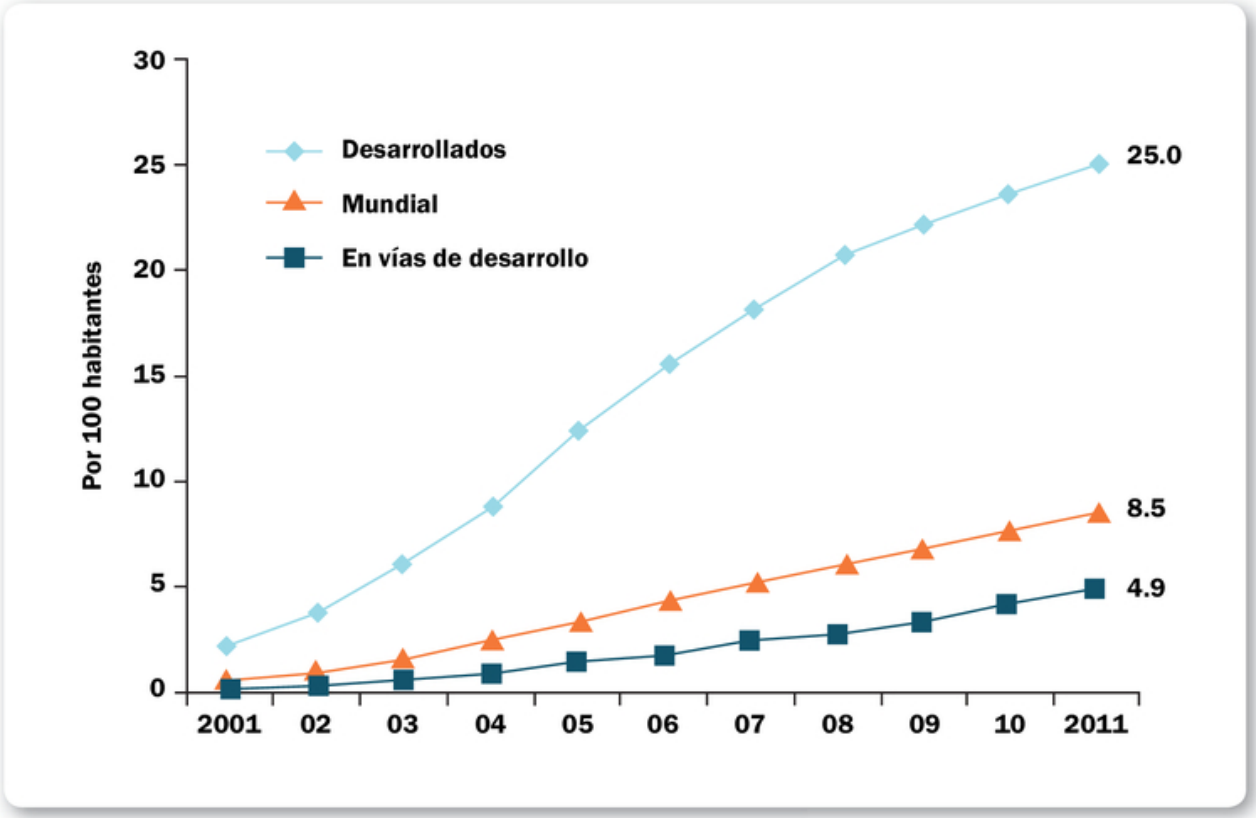


Figura 14. Crecimiento de la telefonía celular durante la primera década del siglo XXI, según estadísticas de **ITU** (**www.itu.int**).

En este escenario **multiconectado**, muchos medios de comunicación extendieron su alcance ampliando sus infraestructuras tecnológicas. Otros, sin embargo, no apostaron desde un principio a Internet y pagaron un alto costo. Pero no solo los grandes medios masivos llegaron a Internet, sino que la red brindó la posibilidad también a medios y **periodistas independientes**, individuos y todos los que quisieran realizar publicaciones.

De esta manera, por primera vez se tuvo la posibilidad de tener virtualmente el mismo espacio para una persona como para un medio, logrando que su lectura dependa de la calidad de los contenidos más que del **lobby** y la **publicidad**.

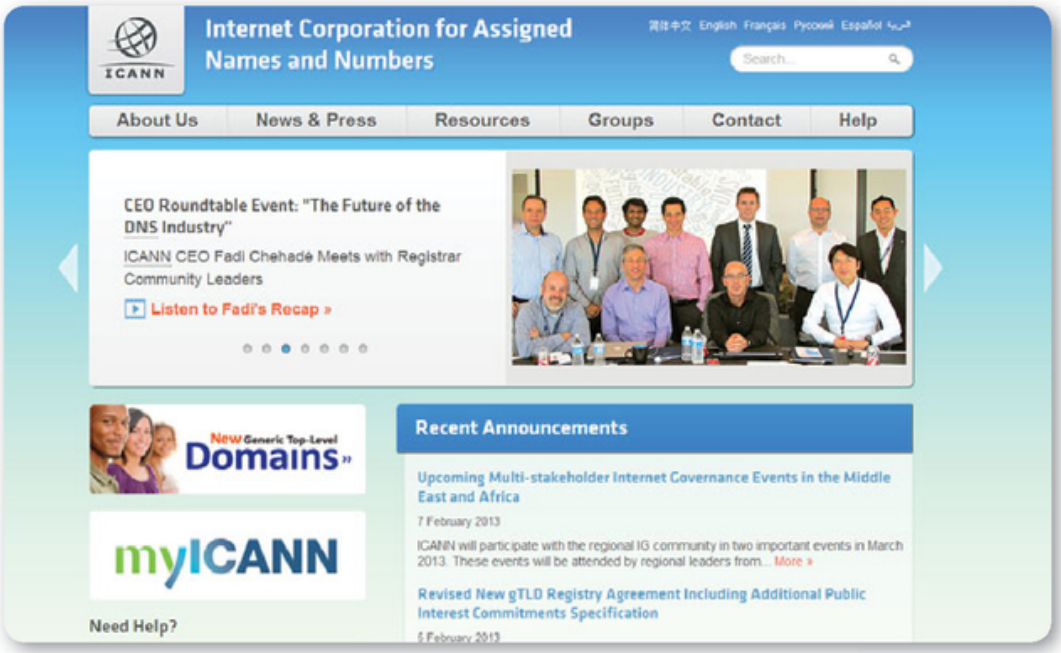


Figura 15. **ICANN** es la organización encargada de gestionar los nombres y números en Internet.

DIRECCIONES A NOMBRES

Cuando accedemos a un sitio web mediante su nombre, la computadora lo traduce a una **dirección IP**, ya que los protocolos y las computadoras solo entienden números. De este modo, se ha logrado evitar que debamos recordar direcciones IP como **74.125.139.102** y podamos acceder mediante un nombre como **www.google.com**. El sistema que permite realizar esta traducción es denominado **DNS** (Domain Name System).

La brecha digital

Considerando Internet como un punto de referencia respecto al avance de la sociedad, comenzó a estudiarse su **penetración** en distintos países para tomarla como un **barómetro** de distintos aspectos del **desarrollo socioeconómico** y cultural. Estos estudios arrojaron resultados por demás interesantes y continúan realizándose en la actualidad, permitiendo, entre otras cosas, hacer una especie de medición de las diferencias entre las sociedades en las que Internet estaba presente y en las que no. Esta diferencia se llamó **brecha tecnológica** o **brecha digital**. En adelante, esta métrica se amplió a las diferencias en la adopción de otras tantas tecnologías de la información y las comunicaciones, como el teléfono celular, la computadora, la banda ancha y otras, tomando como parámetro el estado de desarrollo previo a la adopción.

En función de estos conceptos también se pasó a analizar las diferencias en la **eficiencia** del uso de las tecnologías en base al nivel de **alfabetización**, **accesibilidad** y demás.



Figura 16. El proyecto **OLPC** (One Laptop Per Child) fue el primero de su tipo en combatir la brecha digital en países en vías de desarrollo.

UNA LAPTOP POR NIÑO

En 2005, el profesor del **MIT** (Instituto Tecnológico de Massachusetts) **Nicholas Negroponte** presentó **OLPC** (One Laptop Per Child), una **netbook** de bajo costo orientada a que los niños del tercer mundo tengan acceso a las tecnologías modernas e Internet. Uruguay fue el primer país hispanoparlante en incorporarse al programa con el **Plan Ceibal**, en tanto que Colombia se sumó en 2008 y Argentina en 2011.

Sin embargo, este fenómeno que parece evidente no está del todo reconocido entre los especialistas y estudiosos de la temática, que hacen alusión a las **manipulaciones** políticas relacionadas y a la responsabilidad de las personas en cuanto a su actitud frente a las tecnologías más que a las posibilidades de acceso. En efecto, algunos autores hablan también de **estratificación digital** como un modo de definir más niveles de accesibilidad en lugar de solo dos.

Lo que quizás llama más la atención es la interpretación de la **analogía** que se puede hacer entre el viejo modelo social que marcaba notables diferencias entre personas **educadas** y **no educadas**, y el nuevo medidor que puede distinguir a las personas **conectadas** y **no conectadas**. Otra analogía visible es la serie de estudios realizada en los años 80, que manifestaba duras conclusiones sobre las diferencias entre países desarrollados y en vías de desarrollo en términos de su posibilidad de acceso a las **infraestructuras de telecomunicaciones elementales** de ese entonces, como el teléfono.

Debe tenerse sumo cuidado al hablar de una supuesta **brecha**, ya que se corre el riesgo de aludir a un término que puede suavizar en muchos casos la realidad en virtud de un **nuevo eufemismo**, cuando lo que en verdad se encuentran son verdaderos abismos sociales o cuando el estado más común de las personas es el del **analfabetismo digital**.

RESUMEN

En este capítulo hemos analizado el contexto histórico que acompañó al desarrollo tecnológico y social que nos ha traído hasta el presente para poder comprender las tendencias actuales en estos temas. Hemos pasado de la sociedad de consumo a la de la información y estamos transitando la del conocimiento. Los medios masivos de comunicación han sido de gran importancia en este camino y la llegada de Internet ha marcado un cambio en la manera de relacionarnos con el mundo. Estos avances, sin embargo, produjeron una brecha digital que debemos atender con urgencia si aspiramos a un futuro con igualdad de oportunidades para las generaciones venideras.

Actividades

TEST DE AUTOEVALUACIÓN

1. Encuentre algunas tecnologías que en su propia juventud estaban en desarrollo temprano y hoy utiliza cotidianamente.
2. Determine el impacto que produjo la llegada de la banda ancha (o simplemente de Internet) en su propio hogar.
3. Identifique qué edad tenía cuando tuvo su primer teléfono celular y contrástela con la edad a la que los niños tienen uno propio en la actualidad.
4. Recuerde cuál era la fuente principal de información que consultaba en la infancia o la adolescencia y cuál es en la actualidad.
5. Determine la frecuencia con la que consume información por medio de la televisión, la que lo hace por medio de diarios y revistas y la que lo hace a través de Internet.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

*02

De la Generación X a la Generación Y

En este capítulo comenzaremos a introducir uno de los factores más importantes en la comprensión de los comportamientos de los menores, que es la diferencia generacional. Este será el inicio de un abordaje integral para comprender su mundo y sus necesidades.

- Un siglo de generaciones.....32
- Nativos digitales 37
- Problemas de ayer y de hoy.....39
- Paradigmas obsoletos 42
- El diálogo intergeneracional.....44
- Resumen.....47
- Actividades.....48

Un siglo de generaciones

Muchas veces se habla del término **Generación X** pero no siempre se conoce a qué hace referencia exactamente, sobre todo porque no existe una clasificación científica con fechas precisas sobre los acontecimientos que separan las etapas cronológicas en el mundo. En líneas generales, se denomina **Generación X** a todas las personas nacidas en la generación siguiente a los **Baby Boomers**. Los **boomers**, también conocidos como la **Generación del yo**, se denominaron así por ser quienes nacieron durante el llamado **Baby Boom**, expresión que se refiere a la explosión de la tasa de natalidad ocurrida en determinados países anglosajones en el período que continuó a la **Segunda Guerra Mundial** (entre 1940 y fines de 1960), en virtud de los reencuentros entre los miembros de las familias separadas por el conflicto global. A ellos se les atribuye la expansión de la libertad individual en las sociedades y se los vincula con frecuencia con los movimientos por los derechos civiles y las causas sociales en general.

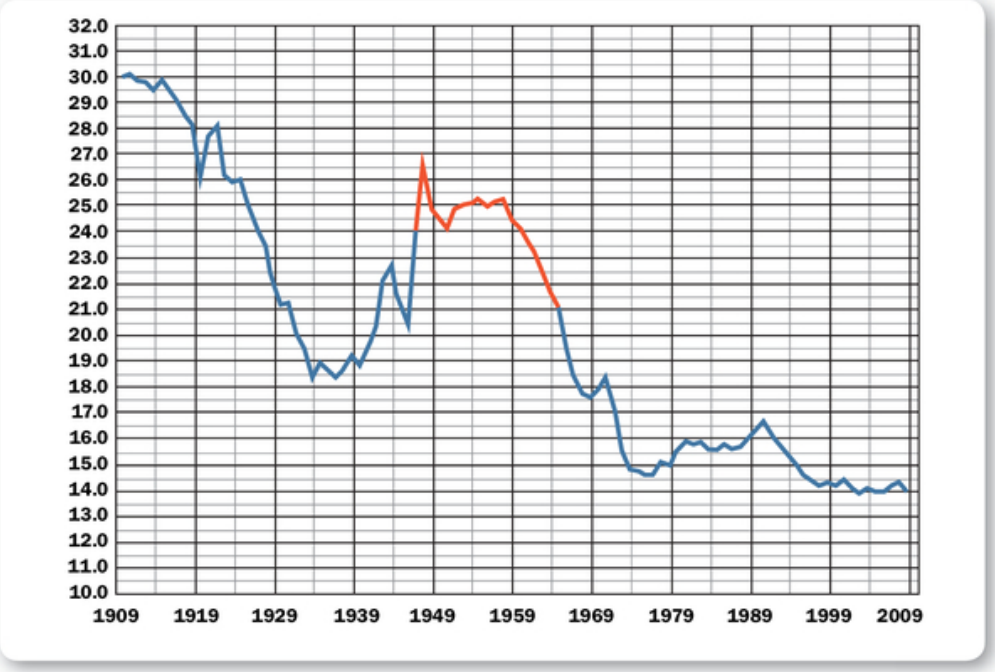


Figura 1. Tasa de natalidad de Estados Unidos por cada 1000 habitantes. En rojo el período del Baby Boom (Fuente: United States Census Bureau).

Volviendo a la Generación X, el término es aplicado comúnmente a las personas nacidas desde 1970 hasta principios de los años 80. Se la ha

nombrado también como **generación de la apatía**, **generación perdida** o **de la rebeldía conformista**. Suele atribuirse a esta generación el hecho de que hayan vivido "de todo" en el transcurso de su vida, desde la televisión en blanco y negro hasta las pantallas de LED y 3D, desde los juegos de mesa más elementales pasando por el nacimiento de los juegos de video hasta las modernas consolas de hoy en día.

El término fue utilizado por primera vez de forma masiva a partir del libro homónimo de los periodistas británicos **Jane Deverson** y **Charles Hamblett** publicado en 1965, pero fue popularizado por el dramaturgo canadiense **Douglas Coupland** en su novela del mismo título. Sin embargo, Coupland consideraba que solo abarcaba a los nacidos entre los años 60 y principios de los 70 y tomaba como referencia a la sociedad norteamericana. En otros países menos desarrollados se considera una extensión mayor en el tiempo e incluso, en Latinoamérica, se ha llegado a especular que los nacidos hasta finales de los 80 todavía contaban con remanentes del mismo impacto social. El concepto continuó creciendo en los medios de comunicación de los 90 para designar a quienes en ese entonces eran adolescentes, lo que les valió el nombre de **Generación MTV**.



Figura 2. El libro **Generación X: cuentos para una cultura acelerada** (1991), de Douglas Coupland, popularizó el término en los años 90.

BOOMERITIS

Muchos **boomers** que han sido figuras públicas o destacadas de su época no se conformaron con realizar pequeños aportes al mundo sino que intentaron siempre que sus creaciones cambiaran radicalmente algún aspecto de la humanidad. Así, su ego los ha llevado a grandes conquistas y grandes catástrofes. La obra **Boomeritis**, de **Ken Wilber**, ilustra con ironía ese narcisismo tan particular.

Las características de esta generación fueron bien marcadas y entre ellas se encuentran, por ejemplo, el hecho de romper las pautas precedentes (esto es normal en los cambios generacionales) pero con énfasis especial en la no creencia en las religiones, las relaciones sexuales prematrimoniales, la depresión e inconformidad, la anarquía en las escuelas y el cambio de rol respecto a la familia y los amigos. Muchos fueron los acontecimientos que signaron la vida de esta generación, como la aparición del virus **HIV**; la explosión del consumo; la aparición de Internet, las computadoras personales y las comunicaciones globales; la caída del muro de Berlín junto al final de la Guerra Fría y la Guerra del Golfo; solo por mencionar algunos de los más significativos.



Figura 3. La caída del muro de Berlín y el final de la Guerra Fría signaron el futuro de los niños de la Generación X.

DEL LIBRO A LA BANDA DE ROCK

Douglas Coupland, autor del libro que popularizó el término Generación X, atribuyó la creación del concepto al músico inglés **Billy Idol**, que había sido parte de la banda de punk del mismo nombre. Esto no fue así ya que Billy Idol había tomado el nombre del libro **Generación X** de **Deverson** y **Hamblett** (1965) que había encontrado en la biblioteca de su madre.

Pero esto no ha sido todo, ya que los nacidos entre principios de los 80 y mediados de los 90 han recibido la posta generacional para llegar a denominarse **Generación Y**, en referencia a la sucesión de la anterior. Ellos llevaron la bandera del **cambio de milenio** mientras atravesaban la adolescencia o la juventud (por eso también se los llama **Millenials**), lo que es un parámetro único en la historia. Los niños nacidos en esos tiempos gozaron de una era de grandes avances ocurridos en muy poco tiempo, y en general crecieron en **entornos más confortables que sus predecesores**, tanto en relación a las condiciones socioeconómicas presentes como en el desarrollo de la tecnología que podía estar a su alcance. Por tal motivo, los nacidos bajo esta generación han aprendido a **adaptarse** muy rápidamente a los **cambios**, hasta el punto en que pueden llegar a necesitarlos como forma de vida, haciendo que impacten en sus trabajos, sus estudios y sus relaciones. Por otro lado, muchos de los elementos que esta generación ha podido disfrutar como productos comunes y basicos de su vida cotidiana son elementos de lujo para sus antecesores inmediatos.

Algo que intensifica este nuevo estado de comodidad, dado principalmente por la tecnología, es el hecho de que es probable que las próximas generaciones no estén sometidas a tantas diferencias sustanciales en ella, de manera similar a lo ocurrido entre esta generación y la anterior. Así, podemos asignar a la Generación Y la característica de haber nacido con **todo a su alrededor**, en contraste con la Generación X que debió esperarlo y verlo nacer. Haber sido la primera generación en vivir sin la existencia de la **Guerra Fría** también impactó en la manera en que sus integrantes concibieron el mundo y, por sobre todas las cosas, ellos acompañaron con su crecimiento el desarrollo de **Internet** y la **informática**.



GENERACIÓN DEL POR QUÉ

La generación Y también ha sido bien conocida como la **generación del por qué**. Esto conforma un juego de palabras en idioma inglés, ya que la expresión **por qué** en inglés (**why**) suena de la misma forma que la expresión de la letra **Y**. Además, coincide con la manifestación del carácter sumamente crítico que se ha encontrado en general en las personas de dicha cohorte.



Figura 4. Los niños de la Generación Y contaron desde pequeños con tecnologías que hoy consideramos básicas.

Los cambios sociales que debieron vivir estuvieron plagados de historias de padres divorciados o solteros y estructuras familiares menos tradicionales que las existentes hasta entonces, lo cual los ha convertido en personas muy abiertas a **escenarios sociales complejos** en busca de soluciones simples.

Como en todas las generaciones, la música y el arte en general han tenido un gran impacto en su crecimiento, y algunos incluso se sintieron representados por los movimientos contraculturales y sus variantes o hasta por tendencias de décadas pasadas.

No podemos olvidar el hecho de que haya sido la primera generación en contar desde su adolescencia con **teléfonos móviles**, **computadoras portátiles** y toda una serie de dispositivos de pequeño tamaño que empezaron a marcar un camino hacia la **miniaturización** de lo que ya existía, además de no necesitar permanecer en una ubicación determinada para poder estar en contacto con el mundo que la rodea.

Esta travesía por la **postmodernidad** ha llevado también a un estado de desencanto que ha dado paso a otras formas de pluralidad y **eclecticismo ideológico** para lograr sobrevivir a la inefectividad de cosmovisiones anteriores, pero el mismo contexto ha dado lugar a una generación acaso más misteriosa y adaptada: los **nativos digitales**.



Figura 5. La extensión de la expectativa de vida actual hizo que generaciones muy diferentes puedan reconocerse y aprender juntas.

Nativos digitales

> LA GENERACIÓN Z ESTÁ ATRAVESANDO SU JUVENTUD EN LA SEGUNDA DÉCADA DEL SIGLO XXI

Nuestra cronología deriva por último en la llamada **Generación Z**, tomada entre mediados de los 90 y mediados de la primera década del **siglo XXI**. Estas personas están especialmente vinculadas a las nuevas tecnologías y han sido consideradas, en gran parte, como una generación impulsiva, consumista y desconfiada. Como consecuencia del escenario en el que han nacido, se las suele denominar **nativos digitales** y, pese a que es clara su existencia y su impacto en el mundo, aún es una generación muy joven que se encuentra en plena formación. Esta generación que está atravesando su juventud en la segunda década del siglo XXI es sumamente **individualista** y está signada por la **dependencia de la tecnología**. Una característica distintiva es que se orienta a relacionarse por medio del mundo virtual, lo que podría derivar en una disminución de las **habilidades sociales**, pese a que, de manera paradójica, puede relacionarse en grandes comunidades online sin siquiera conocerse en persona.



Figura 6. La naturalidad con la que los niños de la Generación Z adoptan la tecnología ha sido objeto de estudio en los últimos años.

El papel que tiene el trabajo en la vida de esta generación es poco importante, ya que sus integrantes aspiran más a la **libertad** que a las **estructuras** y buscan sobrevivir sin los mandatos imperantes, lo que también se refleja en su relación con la educación, que no ven como un camino para mejorar sus posibilidades de crecimiento sino como una **obligación innecesaria** que están dispuestos a evitar en cuanto tengan la posibilidad de hacerlo.

Obviamente, toda la tecnología que tienen disponible ha provocado que la **inmediatez** sea parte de su realidad cotidiana, lo que los transforma en personas muy **impacientes** y marca una tendencia en el mercado de consumo en cuanto a los requerimientos futuros: **velocidad**, **simplicidad** y **comodidad**.

¿NO MÁS LÁPICES?

Algunos especialistas aseguran que, en el futuro, los niños no tendrán necesidad de aprender a escribir en forma manuscrita, ya que todas su interfaces con el mundo contarán con un teclado. Esto, lejos de ser una buena noticia, pareciera predecir que el área del cerebro que se promueve con la escritura ya no será estimulada, de la misma manera que el hombre dejó de saber sobrevivir en la naturaleza.



Figura 7. El uso de teclados y pantallas táctiles en todos los dispositivos hace que la habilidad de la escritura manual se pierda poco a poco.

Llegados a esta instancia, y considerando la cronología presentada, cada uno puede mirarse en el espejo temporal que le corresponde para tratar de comprender mejor el **papel** que cumple y cumplió respecto a sus **antecesores y sucesores**, que si bien puede ser muy evidente, es de hecho lo que nos está dando el gran trabajo de comprender el cuadro general de la sociedad actual de cara al futuro.

Problemas de ayer y de hoy

Los **consejos** que cada generación les dio a sus hijos mientras crecían han cambiado con los años. Seguramente, en alguna época de menos población y más confianza en los barrios y los pueblos bastaba con explicar los **peligros naturales** para prevenir a los niños de posibles problemas comunes, así como también para que se cuidaran de los vehículos que comenzaban a circular por las calles. Luego, hubo un cambio social con el que llegó la **gente malintencionada** de la cual había que protegerse, por lo que los consejos comenzaron a incluir frases como **"no hables con extraños"**. Desde ese entonces, aceptar algo de un desconocido comenzaba a ser peligroso, y esto se sumaba a los consejos de otras épocas.

Muchos podrán recordar las advertencias que sus propios padres les hacían mientras crecían y también recordarán cuándo ellos dejaron de considerarlos niños y comenzaron a tratarlos como jóvenes, con pedidos del tipo **"no olvides usar protección"** cuando se trataba de cierto tipo de salidas.

Hoy, sin embargo, pese a que todos esos consejos de antaño **siguen siendo necesarios**, no bastan para formar en la mente de un niño el sentido común para manejarse en el mundo. Las ciudades han crecido en complejidad al punto de que hasta resulta difícil entender de qué debemos prevenir exactamente a los menores. Como si esto fuera poco, Internet amplió el espectro que hay que cubrir.

Los adultos de la actualidad deben ser conscientes de que muchos de los males que ya eran una amenaza tienen su **correlato en el mundo virtual**. Así, por ejemplo, no hablar con extraños en redes sociales o en chats podría ser equivalente a no hacerlo con una persona frente a frente. Aunque esto podría parecer en principio exagerado, ya que las salas de chat, redes sociales y sistemas de mensajería instantánea ofrecen una aparente sensación de seguridad, si no conocemos quién está del otro lado, en general, **es mejor evitarlo**.

Otra analogía podría hacerse con el **no aceptar cosas de desconocidos**, que podríamos comparar con no recibir archivos o enlaces que tengan una procedencia dudosa o que no podamos garantizar. Un niño que haga clic en una **descarga maliciosa** podría facilitar a un atacante el acceso a su computadora en muy poco tiempo.

También podemos analizar el consejo de **cuidarse al cruzar la calle**, siempre mirar a los costados y estar atento a los arrebatos. En Internet, esto podría aplicarse a la navegación, porque es necesario tener cuidado en los sitios donde uno navega, las páginas que visita y el tráfico que hace circular por su computadora.



CÓMO VENDERLES

Los hábitos de consumo de las nuevas generaciones están siendo estudiados hace tiempo. Sobre la Generación Y se ha determinado que posee gran poder de decisión de compra en sus familias y pondera más las experiencias que los objetos. Venderle requiere comunicación de ida y vuelta, y es más fiel a las marcas con las que se identifica, que, en general, son las que la divierten.



Figura 8. Cuidarse de los vehículos es uno de los consejos más repetidos en la infancia. Hoy, además, es necesario cuidarse del tráfico online.

Otro consejo clásico como el de **no salir sin llaves, dinero y documento** se ha extendido agregando a la lista el teléfono celular, de modo que sea posible la ubicación o un llamado si aparece algún problema. El **no dar información sobre donde vivimos**, que también se nos recomendaba cuando éramos niños, hoy tiene su extensión en no compartir las contraseñas de correo electrónico, el acceso a servicios online, redes sociales y demás. **No abrir la puerta de la casa a quien no conocemos** también se aplica a no permitirles el acceso a nuestra computadora a desconocidos.

De esta manera, podemos entender la Web no como un mundo distinto del real sino como su extensión, donde los consejos de siempre pueden seguir siendo aplicados con algunas salvedades y adaptaciones. Probablemente, las próximas generaciones agregarán **nuevos consejos** a la lista y se volverán naturales los que se gestaron en estos tiempos.

No sabemos exactamente cuáles serán las tecnologías que cambien nuestro modo de pensar el mundo el día de mañana, pero sí sabemos que debemos prepararnos y preparar a los menores para que sus experiencias de la primera infancia y la niñez en el uso de las tecnologías sean **agradables y enriquecedoras**, y que no tengamos que recordarlas por algún mal trago.



Figura 9. Abrirle la puerta a un desconocido es el equivalente físico a dejar que alguien ingrese en la computadora.

Paradigmas obsoletos

Tiempo atrás, la **autoridad implícita** de los progenitores era suficiente razón para que un niño obedeciera sin cuestionamientos. Si lo decía el padre, había que cumplir sin discutir so pena de castigo, que hasta podía llegar a ser físico. Con el recambio generacional, la **autoridad** fue siendo **cuestionada** poco a poco al punto de que para algunas generaciones, no era tan indiscutible la decisión de sus padres a priori, y se atrevían incluso a **desafiarla**. A medida que pasó el tiempo, esto continuó hasta que con la

RITOS DE PASO

Para la **Organización Mundial de la Salud**, la adolescencia es considerada técnicamente como el período que abarca desde los 10 a los 19 años de edad, aunque estudios recientes coinciden en su extensión hasta los 25. La llegada de la adolescencia se ha celebrado en distintas tradiciones con diferentes ritos de paso, como el **Seijin Shiki** en Japón o el **Bar Mitzvah** de la tradición judía.

Generación Z pareciera estar llegando a un límite desde el que podría comenzar a **cambiar la tendencia** o aparecer un elemento que permita reestablecer el equilibrio.



Figura 10. La comunicación con los hijos siempre ha sido un tema complejo para todas las generaciones de la historia.

Como es muy difícil decir **no** a los menores de hoy en día (y en especial a los adolescentes, como ha sido siempre para esa edad), la salida más **salomónica** termina siendo el **diálogo** en casi todos los casos. El problema radica en que esto depende de la **predisposición** de ambas partes. Muchas veces, los padres son quienes no desean llegar a un acuerdo que no sea el cumplimiento de su propia voluntad, a lo que el menor podría **reaccionar** incluso redoblando la apuesta.

De esta manera, podemos comenzar a pensar que el paradigma del **no porque no** es una idea bastante pobre en la actualidad cuando el objetivo es persuadir a un menor de un comportamiento determinado.

Otro de los paradigmas que ya no encuentran tanto arraigo es el del **castigo** del niño **encerrado en la habitación**, ya que el solo acceso a su tablet PC o computadora permite que pueda estar haciendo lo que seguramente haría sin estar castigado. De hecho, cuando los padres se quedan tranquilos porque el menor no está en la calle y está en una habitación, podría estar igualmente en condiciones de ser **engañado** por Internet, como analizaremos en el **Capítulo 4**.



Figura 11. Que un niño esté en su habitación con la computadora e Internet no lo libera de los peligros sociales.

El diálogo intergeneracional

Quizás pueda parecer una obviedad, pero bien sabemos que a lo largo de la historia el **diálogo** entre padres e hijos de cualquier período siempre ha sido un tema **delicado y difícil de abordar**.

El modelo donde una parte cuenta con la experiencia y quiere lo mejor para sus hijos en tanto que la otra parte quiere **descubrir** el mundo por sí misma se ha repetido cada vez y lo seguirá haciendo. Por esto es que encarar la temática del diálogo intergeneracional no es para nada trivial.

Una de las grandes **barreras** que los menores colocan de manera natural entre ellos y sus padres es el hecho de que estos no puedan hablar su **mismo idioma** ni darle la misma **connotación** a las cosas, de modo que su modelo del mundo no es el mismo pese a que digan las mismas palabras. Así, por ejemplo, los adolescentes que vieron nacer el rock & roll lo sintieron como propio, en tanto que para sus mayores se trataba de un estilo nuevo y adoptado que podía gustarles o no, pero que no formaba parte de su **identidad** originalmente.

De la misma manera, con cada generación hubo diferencias entre el mundo que los menores encontraban y aquel en el que sus progenitores habían crecido. En la antigüedad, estos cambios pudieron no ser tan

bruscos, ya que los avances y cambios sociales en otros tiempos eran más **graduales**, excepto en períodos de revolución o guerra, lo que tampoco se daba globalmente sino por regiones, afectando solo a los que allí se encontraban y, a lo sumo, a sus alrededores.

Si tomamos un período de poco más de un siglo hacia atrás, los avances técnicos y sociales han sido tan vertiginosos que, en muchos casos, el mundo en el que crecieron los padres difiere enormemente del mundo en el que lo hicieron los hijos, generando que las brechas del **lenguaje** y el **uso cotidiano** de las cosas se ampliaran.

En lo que a las nuevas generaciones se refiere, este tema se ha intensificado aún más, y nos encontramos con lo que hoy tenemos en escena: padres que nacieron con la **radio** y la **televisión** en blanco y negro y crecieron con el paso a la TV en color y la llegada de Internet y los celulares junto a niños que nacieron con la TV en color, Internet y las **comunicaciones móviles** y crecieron con las **redes sociales**, la **banda ancha** y los **smartphones**.



Figura 12. Utilizar la tecnología para acercarse a los menores los hace sentir que hablamos su mismo idioma.

El problema que se plantea con esto no es tanto la adaptación de los padres y los educadores a las nuevas tecnologías sino el hecho de conseguir que los menores los consideren **figuras de autoridad**. Esto queda bien claro cuando los niños se encuentran con adultos completamente migrados desde su entorno de origen al actual, ya que

los niños conocen tanto como ellos o más sobre **Facebook**, **Windows Live Messenger**, **Skype**, **iPhone**, **tablet PCs**, etcétera. El resultado en los menores es sorprendente, ya que de inmediato suelen comportarse todos de la misma forma: **quieren aprender**. Mientras los más cercanos a la adolescencia quieren **poner a prueba** a los adultos, lo cual es normal para ellos por la edad, pero en general el menor encuentra una salvaguarda en el mayor por el hecho de hablar su mismo **idioma**.



De otra manera, un menor puede mirar a sus padres que le aconsejan sobre Facebook sin siquiera tener una cuenta activa y pensar: **"¿Cómo me dice lo que puedo hacer y no hacer si ni siquiera sabe de qué se trata?"**.

Figura 13. Compartir momentos tradicionales que no incluyan tecnología puede ayudar a reforzar mucho los vínculos con los niños.

Curiosamente, los niños son muy **sensibles** para detectar las **incongruencias** en los padres. Si estos dicen algo y hacen otra cosa, piensan algo y dicen lo contrario o tienen cualquier inconsistencia en su personalidad o manera de actuar, el niño las detectan rápidamente y **actúa en consecuencia**, manifestando por lo general **rechazo** y **crítica**, pensando en su interior: **"Si ellos no actúan conforme a lo que dicen ¿por qué debería hacerlo yo?"**.

CAMBIOS Y MÁS CAMBIOS

La adolescencia es una gran etapa de cambios físicos y psicológicos que marca la transformación del niño en joven adulto. En el comienzo aún carece de una identidad definida y autonomía individual, por lo que va en su búsqueda. Aquí se manifiesta su capacidad afectiva y las emociones relacionadas con el amor, y comienza a elegir a sus amigos por afinidad.

Los niños encuentran estas incoherencias aunque no sepan expresarlo con palabras y de alguna manera nos harán saber aquello que los hace dudar y que los lleva a pensar que ese es el comportamiento que deben modelar para su madurez.



Figura 14. La adolescencia se caracteriza por la rebeldía natural en favor de la búsqueda de la identidad.

Hoy en día, el **diálogo** entre menores y adultos se basa en un gran esfuerzo de los padres para **meterse en el mundo en el que los niños están creciendo**, comprendiendo las cosas como ellos las entienden, aprendiendo a manejar sistemas, software y dispositivos y, por sobre todo, teniendo una grandísima cuota de **paciencia**.

RESUMEN

En este capítulo hemos visto cómo se fue dando el traspaso de una generación a otra a través del tiempo, comenzando el análisis por los **Baby Boomers**, pasando por las **generaciones X**, **Y** y **Z**, estos últimos llamados **nativos digitales**. También entendimos cómo muchos de los antiguos consejos ya no alcanzan para quedarnos tranquilos ya que el escenario ha cambiado y con él las costumbres y la manera de relacionarnos. Luego, analizamos algunos paradigmas básicos que también requieren ajustes o cambios para ser utilizados hoy en día, y describimos brevemente algunas pautas que marcan la eficiencia en el diálogo entre padres e hijos.

Actividades

TEST DE AUTOEVALUACIÓN

1. Identifique a qué generación corresponden las personas del entorno cercano.
2. Busque fotos de su infancia y compare los elementos presentes con respecto a las fotos de los menores actuales.
3. Reconozca cuáles eran los elementos electrónicos del entorno en el que creció y cuáles de ellos ya no se utilizan o no existen.
4. Averigue cuáles eran los consejos que le daban los padres a sus padres en la infancia.
5. Determine la cantidad de tiempo que los menores de su familia pasan a diario con la televisión en comparación con el que pasan con las computadoras.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

*03

El escenario virtual

Navegadores, buscadores, portales de noticias, redes sociales, blogs y demás. El escenario virtual plantea un contexto particular que debe comprenderse en profundidad para luego abordar otras temáticas más complejas.

- Vida online y lenguaje escrito . 50
- Redes sociales 53
- Mensajería instantánea y chat 57
- Juegos de consola y online 59
- La identidad virtual 62
- La nube y la información 65
- Resumen 67
- Actividades 68



Vida online y lenguaje escrito

Desde que existe Internet, muchas personas comenzaron a considerar la existencia de una **identidad virtual** separada de la real, de modo que si bien podría suponerse que ambas deberían ser dos caras de la misma moneda, no terminó siendo así. En efecto, muchas de las personas que se vieron atraídas por el **universo virtual** eran, justamente, aquellas que adolecían de limitaciones en las **habilidades sociales**, por lo que encontraron allí un espacio para expresarse, interactuar y compartir sin la imperiosa necesidad de tener que modular de manera correcta o aprender a manejar el lenguaje gestual.

Esto dio origen a un modo distinto de comunicarse, **completamente por escrito**, que a su vez derivó en un fortalecimiento de las **capacidades literarias** y de escritura general para algunos y una necesidad de adaptación forzada para otros. Este modo de comunicación permitió dar un salto a nivel social en la forma tradicional de **expresión escrita** por medio de cartas o máquinas de escribir, pero también ofició de barrera para aquellos que a priori no se sentían cómodos con la escritura en sí.

Así sucedió que algunos comenzaron a **deformar el lenguaje** para adaptarlo a su manera de expresarse, comenzando por **alterar palabras** para reducir su extensión y **acelerar la comunicación**. En un comienzo, tales deformaciones o modificaciones obedecían a un uso finamente irónico de la propia lengua, por lo que en general las personas que lo hacían solo estaban **jugando con las palabras**. Con el tiempo, mucha gente empezó a utilizar deformaciones en las palabras no por erudición literaria sino por error, omisión o apropiación de comportamientos que los hicieran parecer diferentes. Esta notoriedad aparente dejó así de ser terreno de algunos para pasar a ser caldo de

CORRÍJAME, MR. SOFTWARE

Los avances en el software de procesamiento de textos (como **Microsoft Word**) permitieron obtener resultados muy superiores a los que se obtenían antes en cuanto a los errores de escritura, pero promovieron una cultura de la comodidad en la que la gente se acostumbró a escribir sin pensar porque el software lo corregiría después. El problema, claro, reside en la conciencia del uso.

cultivo de muchos para la **deformación de la lengua**, que también se extendió a los otros dispositivos electrónicos donde se ingresan letras, como los teléfonos celulares y demás. En el caso de los teléfonos móviles, la **necesidad de abreviación** era más requerida por las **limitaciones del medio**, lo que contribuyó fuertemente a potenciar el uso personalizado de las palabras y las expresiones, algo que se reflejó en la formación de una lengua propia compuesta por argots.

Emoticón textual	Significado	Emoticón gráfico
---	---	
:(/ =(/ :/	Tristeza, decepción	
:D / =D / xD	Sonrisa	
8)	Gafas o lentes de sol	
;)	Parpadeo, guiño	
:* / =*	Beso	
:x / =X	Boca cerrada (secreto) o insatisfecho	
:o / =O	Cara de sorpresa	
T.T / Y.Y / ='(/ :'(	Lágrimas	
sz / S2 / <3	Corazón, amor	

Figura 1. Los emoticones permiten expresar emociones por medio de la representación, con caracteres de caras y gestos humanos.

La limitación en el canal de comunicación dada por la lengua escrita promovió la invención de los emoticones (**emoticons**), símbolos de dos o tres caracteres que reflejan un **estado de ánimo** por la apariencia similar a la de una cara con esa expresión. Los emoticones permitieron ampliar la expresión escrita, agregando cierto **contenido emocional** a las palabras, y mejorando así la calidad del mensaje en muchos casos.



Figura 2. El lenguaje escrito, mandatorio en el mundo virtual, permitió diagnosticar problemas educativos más profundos.

El resultado de esta **transformación** en la manera de comunicarse por la necesidad de escribir puso de manifiesto, además, muchos **problemas de escritura**, en especial de niños y adolescentes que, por carecer de educación suficiente, no habían aprendido a expresarse correctamente por escrito. Esa fuerte secuela de una **pobre educación inicial** llamó la atención de muchos y fue ignorada por otros, pero es hoy en día el signo más claro de la ineficiencia de los sistemas educativos.

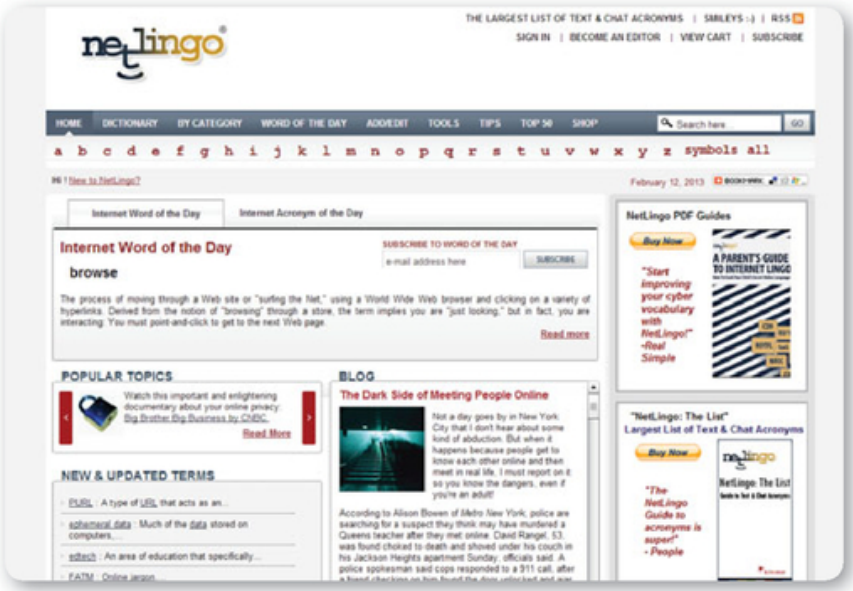


Figura 3. **NetLingo** (**www.netlingo.com**) es un sitio muy útil que provee información sobre el lenguaje usado en Internet.

En especial en las poblaciones más pobres, los errores que se encuentran en muchos niños y jóvenes al escribir no se limitan solamente a la **ortografía**, sino que también llegan hasta la gramática, la semántica y la sintaxis. Esto hace sospechar de inmediato que existen **inconvenientes previos** que parten de la manera de construir las frases en su mente, con lo que el problema incluso **trasciende la educación** y pasa a tratarse de una dificultad en la etapa de formación de su sistema neuronal, algo que puede atribuirse a enfermedades, mala alimentación o desnutrición, flagelos que en el **siglo XXI** no pueden darse el lujo de existir, aunque lo hagan.

Redes sociales

Una **red social** es una estructura en la que hay individuos y relaciones entre ellos, y puede ser de diversos tipos. Al surgir distintos sitios web que brindan la funcionalidad de interconectar personas nacen las redes **sociales virtuales**, que son un **vehículo** para conectarse con amigos, conocidos, colegas y más. Estas redes se basan en la idea de que todos podemos estar potencialmente conectados con todos a través de los **contactos de contactos**.

Sin embargo, estos sitios también tienen un lado negativo. Una de las razones por las que los sitios de redes sociales han pasado a ser tan peligrosos es el hecho de que puedan incluirse **aplicaciones de terceros**, que no son fáciles de controlar por las mismas redes, haciendo que se conviertan en un vehículo para la distribución de contenidos no deseados y código malicioso. Una idea para evitar este problema sería detener el desarrollo de aplicaciones, pero esto

CAMPAÑA DE AMISTAD

En 1963, la fusión de dos empresas estadounidenses provocó miedo de despidos y reformas entre su personal, por lo que se decidió realizar una acción de marketing llamada **Campaña de amistad**. Para esa campaña, el diseñador gráfico **Harvey Ball** diagramó, en diez minutos, la famosa carita sonriente por US$ 45. La imagen, caída en el dominio público, derivaría en el más famoso de los emoticones: **:-)**.

le restaría cierto atractivo a los sitos. También se podrían supervisar todas las aplicaciones, aunque esto agregaría un costo operativo bastante alto a la existencia de la red.

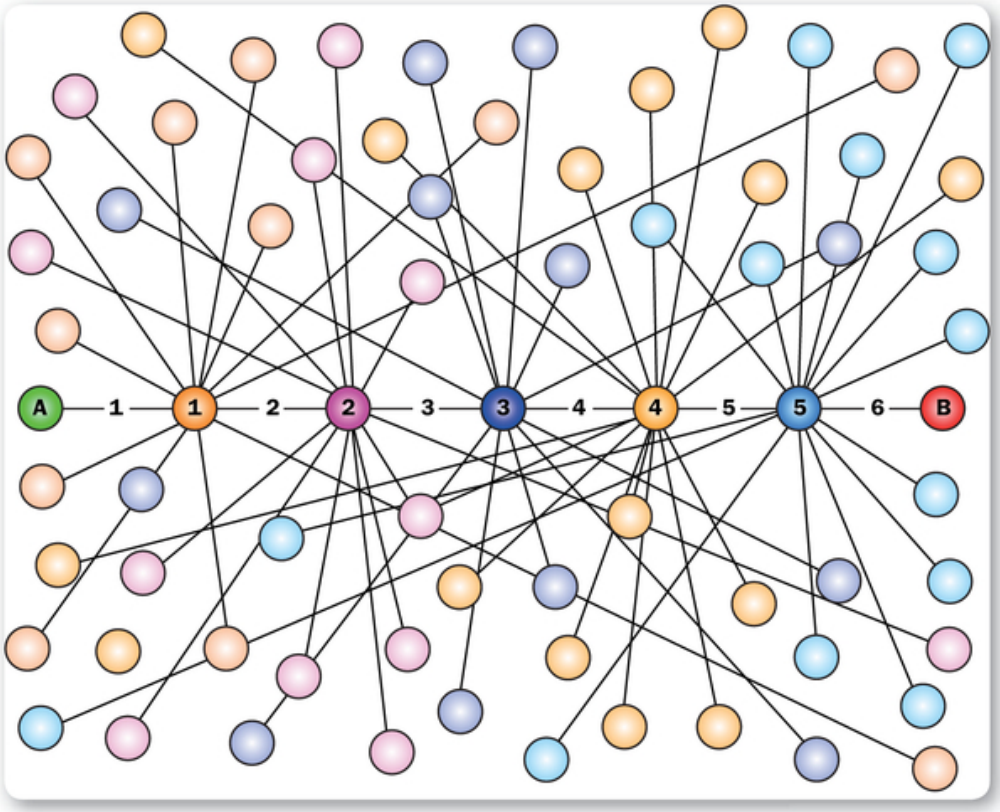


Figura 4. La teoría de los **6 grados** afirma que todas las personas estamos separadas por un máximo de seis contactos conocidos.

Por otro lado, curiosamente, existe una **falsa economía de la confianza** según la cual la gente no daría sus datos personales a desconocidos en la calle, pero los dejaría en un sitio web a través de **perfiles** personales. Cada persona deberá analizar los riesgos que



EMOTICONS Y VERTICONS (¬¬)

Así como los emoticones representan expresiones de emociones de rostros y se pueden leer girando la cabeza, con el tiempo surgieron los **verticons**, que son expresiones de rostros para las que no es necesario girar la cabeza por estar representadas en sentido vertical. También se los conoce como emoticones japoneses o **kaomoji**, y se encuentran con frecuencia en el **manga** y el **animé**.

implica estar presente en los sitios web y la **privacidad** que ofrecen las redes en función de sus contratos, incluyendo las que cuentan con opción de **membresía paga**.

Dado que es deseable evitar que se puedan realizar deducciones a partir de nuestros datos, es necesario ser prudentes con nuestras contraseñas y no manejar para todos los servicios, sistemas y sitios un único par **usuario/clave**. Esto es especialmente grave ya que muchas veces la **fuga** de datos no se genera por nuestros propios perfiles sino por los de nuestros contactos, que con inocencia agregan información en apariencia inocua, que, al ser correlacionada con la de otros usuarios de nuestra confianza y los de otros, puede generar un gran caudal de datos útiles para cualquier posible usuario malintencionado.



Figura 5. **LinkedIn** es la red social de negocios más grande del mundo.

Las redes sociales no brillaron por su popularidad desde el comienzo sino que fue con el estallido de **Facebook** que muchos encontraron su puerta de entrada a ellas. Facebook, que se estima alcanzó los 1000 millones de usuarios durante 2012, permitió materializar la **teoría de los 6 grados** de separación como nunca antes había ocurrido, pero a la vez sirvió como vía de acceso a nuevos peligros propios de este tipo de redes, sobre todo teniendo en cuenta sus siempre cambiantes políticas y sus términos y condiciones de uso. Esto también fue potenciado por el creciente acceso a Internet desde

los teléfonos celulares y por la inclusión de las **Fan Pages** o páginas de fanáticos, que permitieron a las marcas interactuar con sus usuarios de manera directa. Considerando la importancia de Facebook y las redes sociales, iremos mencionando sus distintos aspectos, los cuidados que debemos tener y los consejos por seguir en los **capítulos 4**, **5** y **6**.

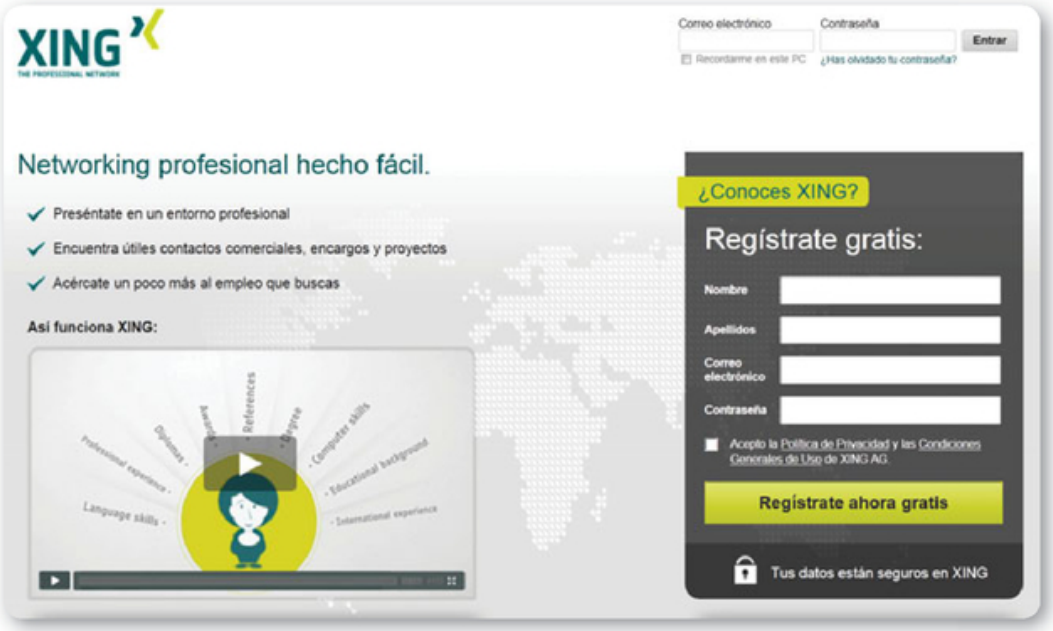


Figura 6. **XING** es la red social de negocios más importante de Europa.

Existen otros tipos de redes que sin ser menos importantes son tal vez menos populares. Se denominan redes de **microblogging** y, entre ellas, la más famosa es **Twitter**, la red social del pajarito. Twitter solo permite escribir mensajes de hasta 140 caracteres y los perfiles de usuario son muy simples, admite solo una imagen de perfil y una breve descripción. El tipo de usuarios que se inclinan hacia el uso de este tipo de redes es distinto al de Facebook, ya que estas proveen la posibilidad de consumir información de una manera muy eficiente mediante la selección de personas a quienes seguimos, que no necesariamente deben seguirnos. Este esquema de **seguidor** (**follower**) y **seguido** (**followed**) promueve su uso por parte de artistas, famosos, políticos y otras figuras que tengan un diálogo mayormente unidireccional con su público objetivo.

> TWITTER PERMITE CONSUMIR INFORMACIÓN DE MANERA MUY EFICIENTE

Mensajería instantánea y chat

Se conoce como **mensajería instantánea** (o **IM** por **Instant Messaging**) a los sistemas de **chat** (**charla virtual**) entre dos o más personas, donde el texto se escribe de una ventana individual a otra, cada una con su interfaz. A diferencia del e-mail, estas conversaciones se dan en **tiempo real**. Esto requiere un software cliente que se conecta a un servidor donde todos los demás clientes se conectan. Esta conexión se realiza de manera **transparente para el usuario**, por lo que no se requieren habilidades particulares para su uso, solo instalar el programa, ejecutarlo, tener una **cuenta válida** y acceder.

Algunos de los servicios más conocidos de IM han sido **ICQ**, **Yahoo! Messenger**, **Windows Live Messenger**, **Pidgin**, **Google Talk** y **AIM**, aunque la tendencia ha cambiado. En el principio, ICQ dominaba el mercado y luego fue **MSN Messenger** (renombrado Windows Live Messenger). Por su parte, **Google Talk** avanzó fuertemente en los últimos años debido a que muchas personas contaban ya con servicios de Google como **Gmail**, **Google Calendar**, **Google Tasks**, etcétera. A fines de 2012, Microsoft anunció el **final** del ciclo de vida de Windows Live Messenger, en favor del desarrollo del recién adquirido **Skype** que, para principios de 2013, comenzó a ofrecer opciones de migración de **lista de contactos**.

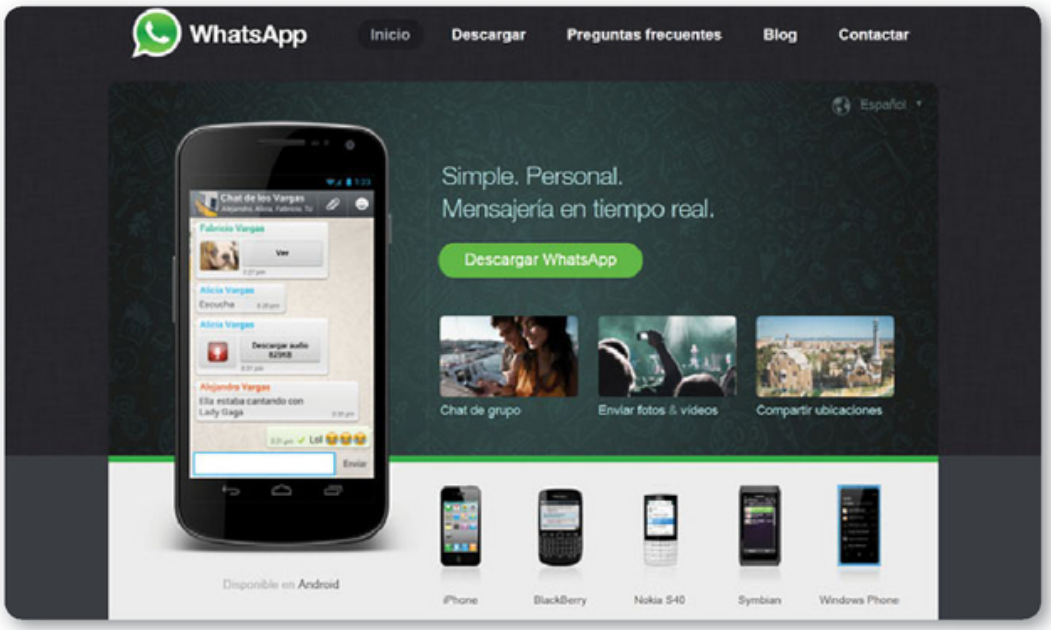


Figura 7. Pese a su cuestionada seguridad, **WhatsApp** es una de las opciones más utilizadas para el chat entre móviles.

Los sistemas de IM suelen ofrecer, además de intercambio de mensajes, **envío de archivos**, conversaciones de **voz y video**, **juegos en red** y otras funciones, de modo que gran parte de la interacción entre personas conectadas a diario se da entre los que conforman la lista de contactos del mismo sistema.

También hay programas que permiten el acceso simultáneo a **varios sistemas de IM**, función que comenzaron a incluir algunos productos oficiales con el tiempo. Una gran ventaja de contar con varias cuentas en una sola aplicación es que se consumirán menos recursos del equipo.

Quizás el último grito de la moda en la mensajería lo ha querido dar **Facebook** con su mensajero interno, pero pese a ser la red social más grande del mundo **no ha sido del todo bien recibido**.

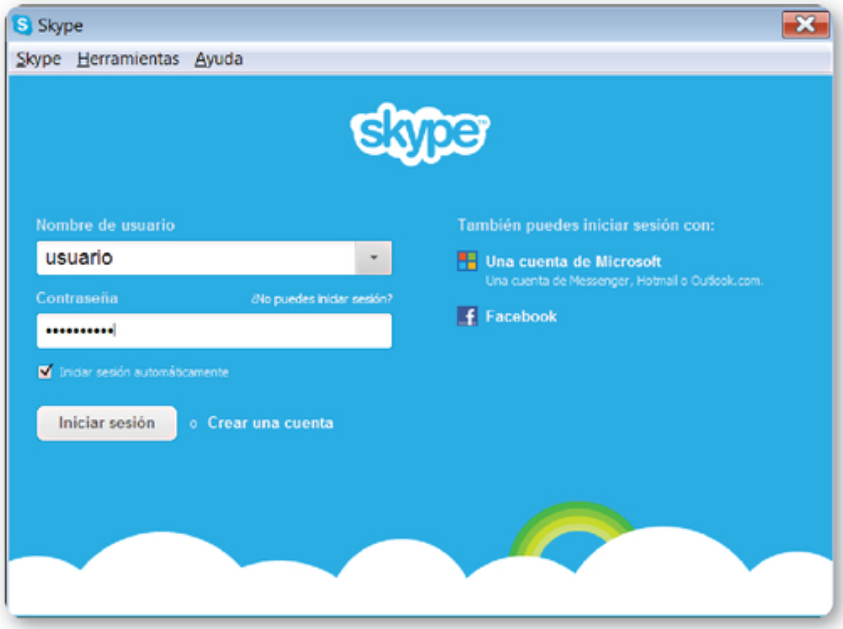


Figura 8. Skype es un sistema de videollamadas por Internet, mensajería instantánea y videoconferencias grupales, desde casi cualquier dispositivo.

JERGA DE INTERNET

La jerga específica de Internet, también llamada **cyber-slang**, **netspeak** o **chatspeak**, incluye abreviaciones, acrónimos y anglicismos que buscan la reducción del texto escrito. Los **argots** son un factor de renovación lingüística y si bien antiguamente estaban asociados a la vulgaridad y a la poca cultura, en la actualidad son estudiados para comprender las dinámicas sociales.

Sumado a esto, los sistemas de mensajería específicos para dispositivos móviles, como **WhatsApp** o **BlackBerry Messenger**, también encontraron su nicho ya que mejoraron la eficiencia de las comunicaciones respecto a las versiones móviles de los programas que existían para la computadora.

Es de esperar que con tanta posibilidad de conversar con amigos, conocidos y compañeros, la mensajería instantánea sea **el medio preferido** por las nuevas generaciones.

Juegos de consola y online

Los juegos no podían quedar afuera de un análisis que incluya a los menores, aunque, curiosamente, el **rango etario** que más consume juegos es el de la Generación X, lo que se cree que se debe a que fueron sus primeros consumidores cuando eran niños. Esta tendencia facilita la comprensión de los padres de más de 30 años de los niños de las generaciones Y o Z, siendo así uno de los **conectores** más importantes de encuentro y **espacios comunes** para **compartir** entre padres e hijos.



Figura 9. Además de entretenernos, al utilizar los juegos de video en familia podemos conectarnos con los menores en su propio terreno.

Los juegos de video tienen **distintos segmentos**, pasando por los ya clásicos de **consola**, los de **computadora** y los de **teléfonos móviles**. De manera transversal, podemos considerar también los **basados en Internet**, que muchas veces pueden jugarse desde **distintas plataformas**.



Figura 10. **Club Penguin** es uno de los juegos online elegidos para los más chicos.

Las consolas de video juegos, como **Microsoft Xbox**, **Nintendo Wii** y **Sony Playstation**, ofrecen una plataforma diseñada para jugar de modo individual o en grupo. Los juegos de PC pueden ser más exigentes, dada la tecnología de placas de video y los procesadores actuales. Los **juegos para celulares** aprovechan los potentes procesadores incluidos en la actualidad en los dispositivos móviles, aunque muchas veces con juegos muy **sencillos** se logra acaparar lo suficiente la **atención del usuario**.

SALAS DE CHAT

Antes de la popularización de los sistemas de mensajería instantánea, los usuarios se encontraban en **salas de chat**, espacios virtuales creados en servidores de **IRC** (**Internet Relay Chat**) que proveían servicios, por lo general libres y gratuitos, para facilitar las comunicaciones públicas o privadas entre usuarios, aunque también había salas y servidores cerrados.



Figura 11. **Mundo Gaturro** es otro de los juegos online preferidos de los menores.

Sin embargo, se ha dado un curioso fenómeno con los juegos online, ya que pese a su **limitada calidad gráfica** algunos han hecho gran furor. Existen juegos creados específicamente para Facebook, donde los usuarios pueden jugar y relacionarse con otros miembros de la red.

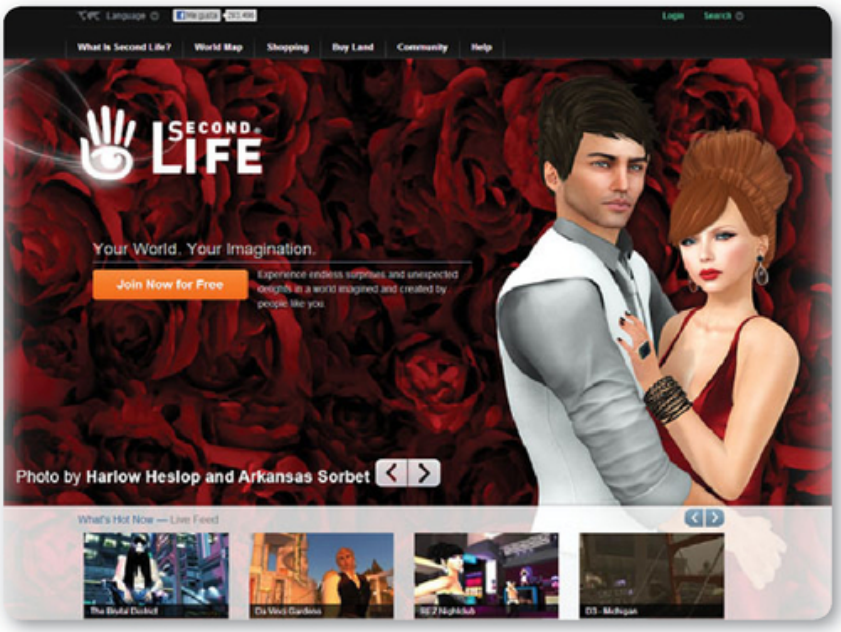


Figura 12. **Second Life** es un juego que permite vivir en un mundo virtual donde hasta existen actividades comerciales vinculadas al mundo real.

Los peligros potenciales para los menores asociados a los juegos están en su mayoría vinculados a las redes sociales y los juegos online, dado el **riesgo inherente** que existe en la **interacción** entre los distintos jugadores, en especial con aquellos que cuentan con funcionalidades de **chat directo** entre ellos, ya que es difícil asegurar quién está del otro lado y sus **intenciones**. Además, la utilización de **moneda virtual** también puede ser problemático cuando se trata de menores de edad.



Figura 13. En **Facebook** son populares los juegos como **CityVille** y **FarmVille**, propios de la plataforma, que atraen millones de usuarios.

La identidad virtual

Hay quienes sostienen que existe una identidad virtual distinta y desligada de la real porque el entorno en el que esa identidad opera es completamente diferente, pero lo cierto es que no lo es tanto. El vínculo entre nuestras **actividades online y offline** es cada vez más sutil y se desdibuja conforme vamos estando más conectados. En muchos casos, nuestra información personal se encuentra online sin que nosotros mismos lo hayamos **autorizado explícitamente**, y puede darse por diversos motivos, como el estar incluidos en contratos

publicados en un boletín oficial, en bases de datos ilegales, padrones que contienen información de los ciudadanos o por cosas que un tercero haya escrito sobre nosotros.



Figura 14. Hay veces que encontramos en Internet información sobre nosotros mismos que atenta contra nuestra privacidad.

Es importante conocer **qué información tiene Internet sobre nosotros**, lo que podemos realizar de manera sencilla buscándonos a nosotros mismos en **Google** o **Bing**. Este simple ejercicio puede darnos un punto de partida en la averiguación de nuestros propios antecedentes digitales. En el caso de encontrarnos irremediablemente en los buscadores, es necesario determinar **en qué condiciones aparecemos**.

También es posible quedar asociados a personas con el mismo nombre, lo que puede confundir a quien nos busque, o encontrar

PÁJAROS ENOJADOS

Si hay un juego que revolucionó a las masas es **Angry Birds** (Pájaros enojados), creado en el año 2009 por **Rovio Mobile**, una empresa de Finlandia. Ha tenido más de mil millones de descargas en 2012, convirtiéndose en el juego más vendido de la historia para dispositivos móviles. Además, se crearon juguetes físicos de los pájaros, disfraces y toda clase de **merchandising**.

un **homónimo** que se dedica a actividades ilegales y aparece en nuestros mismos **resultados de búsqueda**. Aunque no podemos evitar que esto suceda, es mejor saberlo.

Cada uno tendrá en Internet un **perfil** conformado por la **suma de la información** que se encuentre sobre uno. Seguramente, si tenemos un **bajo perfil** en lo cotidiano tendamos a tenerlo también en la Web, en cambio el **alto perfil** y la extroversión suelen permitir la exposición de más información propia.

Con los menores y los jóvenes se ha dado un fenómeno curioso en los últimos años: la **tendencia generalizada a querer aparecer en Internet** sin tener en cuenta las consecuencias presentes y futuras. Si a esto le sumamos la masificación de las **cámaras digitales** y su inclusión en teléfonos celulares, la información ya no será solo texto escrito sino también **imágenes y hasta videos**. Esto ha dado por percibirse en la Web como un **foco de popularidad** que se traduce a la vida cotidiana en muchos casos, tal como ocurre con la televisión, donde mucha gente se desvive por aparecer con el objetivo de obtener **fama y reconocimiento**.



Figura 15. Muchas decisiones sobre las personas se toman hoy basadas en su identidad virtual y sus perfiles online.

Estar en Internet es equivalente a **pertenecer al mundo actual**. De hecho, en el ámbito corporativo es sabido que las empresas que no figuran en la Web están perdiendo terreno comercial, y esto podría costarles caro sobre todo si sus competidores sí la utilizan.

¿DÓNDE ME ANOTÉ?

Una de las malas prácticas más comunes es no llevar registro de nuestra participación en sitios web. Muchas personas se suscriben a redes sociales, listas de correo, noticias y boletines, novedades de blogs y páginas con **RSS** y después olvidan su participación. Luego, cuando comienzan a recibir **spam**, se preguntan de dónde se obtuvo esa información.

Una cualidad de este tema es que se debe manejar una solución de compromiso entre la **necesidad de estar online**, visible y presente, pero a la vez estar seguro, protegido y que no se **utilice maliciosamente** nuestra información. Algunos especialistas afirman que no es conveniente contar con perfiles online, aunque otros asumen que si el riesgo ha arribado para quedarse, será solo cuestión de tiempo tenerlo, por lo que prefieren **tener presencia online** aunque más no sea para **reservar su nombre** y evitar así el **robo de identidad**.

En suma, **no existe una identidad virtual separada de la real**, sino una sola identidad personal que tiene un aspecto digital y uno físico, pero ambos conforman la **vida real**.

La nube y la información

La **computación en la nube** o **cloud computing** es un **paradigma** en el que la información es almacenada en servidores conectados a Internet y los equipos cliente la reciben desde su ubicación. Si bien el concepto se ha utilizado por años sin nombre característico, la idea cobró especial relevancia cuando grandes empresas, como **Google**, **Amazon** o **Microsoft**, comenzaron a construir su propia infraestructura online, lo que derivó en el crecimiento masivo de sistemas que proveían diferentes recursos para la prestación de servicios a gran escala.

La nube, como se la llama comúnmente, permite la existencia de servicios a nivel mundial con mínimos tiempos de caída, además de otros beneficios tanto para sus prestadores como para los usuarios. Su principal desventaja es la dependencia del acceso a Internet, que limita su disponibilidad en ciertas ubicaciones.

Por un lado, una de las clasificaciones que se utilizan en las nubes distingue las **nubes públicas** (controladas por terceros), donde el usuario final no sabe lo que ocurre en el servidor o red en el que opera; y las **nubes privadas**, en las que se puede conocer y definir el acceso a la infraestructura y los recursos. Además, existen las **nubes híbridas** como combinación de las anteriores. Por otro lado, la nube cuenta, básicamente, con tres capas de funcionamiento a nivel de servicios: la más cercana al usuario, que es **software como servicio** (como los

webmails, **Microsoft Office 365** y **Google Docs**); la capa intermedia, que es **plataforma como servicio** (como **Microsoft Windows Azure** y **Google App Engine**), y la más cercana al hardware, que es **infraestructura como servicio** (como **Amazon Web Services**).

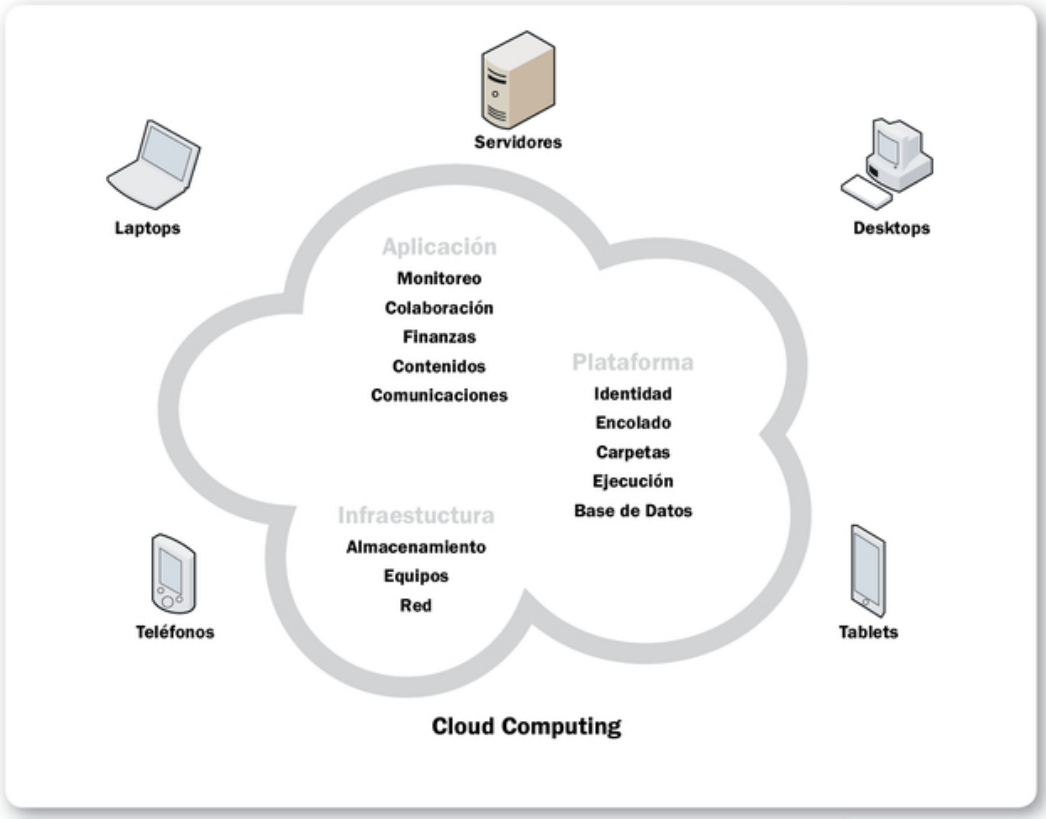


Figura 16. Esquema de funcionamiento de los servicios en la nube.

Normalmente, los usuarios se relacionan con la capa de servicios, utilizando **funcionalidades** brindadas de manera **gratuita** por grandes empresas de tecnología. Este curioso detalle de que algo tan útil pueda ser gratuito debe contrastarse con el hecho de que, al

SERVICIOS POPULARES EN LA NUBE

Algunos de los servicios basados en cloud computing de uso cotidiano son, por ejemplo, los que permiten el almacenamiento de archivos en línea para poder tener siempre disponible nuestros datos desde cualquier ubicación. Ejemplos caracterísiticos de estos servicios son **Dropbox**, **Google Drive**, **iCloud** (**Apple**) y **SkyDrive** (**Microsoft**). En general, cuentan con versiones gratuitas y pagas.

utilizar servicios online, estamos **dejando toda nuestra información en manos de un tercero**. Esto no es en sí mismo algo malo, pero debemos tenerlo en cuenta si lo que hacemos circular por ese entorno es **información confidencial** muy privada.



Figura 17. **Dropbox** es uno de los servicios más populares y completos de almacenamiento de datos en la nube.

En efecto, podemos ilustrar esto mismo en palabras del controversial fundador de la **Free Software Foundation**, **Richard Stallman**, que afirma que la nube pone en peligro las **libertades de los usuarios** y que podría tratarse de una trampa comercial para obligar a la gente a usar sistemas propietarios. Contestatario tal vez, pero poco sorprendente sin duda.

RESUMEN

En este capítulo hemos comenzado con el análisis del contexto virtual que corresponde a Internet y la tecnología, que debemos comprender con profundidad para reconocer el mundo en el que crecen hoy los niños. Así, analizamos las implicancias de una vida online y una identidad digital, junto al impacto de las redes sociales y los sistemas de mensajería instantánea en cuanto a los nuevos canales de comunicación que conforman. También comprendimos el rol de los juegos de video como herramienta de entretenimiento de los menores y por último, conocimos el concepto de computación en la nube, que a diario utilizamos, incluso antes de saber de su existencia conceptual.

Actividades

TEST DE AUTOEVALUACIÓN

1. Busque en Google su nombre completo entre comillas (para que devuelva la búsqueda exacta de los términos) y sus variantes (nombre completo, apellido y nombre, nombre y apellido, etcétera) y analice los resultados.
2. Identifique las palabras que usa en el lenguaje escrito que son deformaciones o abreviaciones del idioma español. También reconozca los anglicismos que utiliza.
3. Analice la diferencia entre las redes sociales profesionales y de negocios, y las de entretenimiento y amistad, navegando por los distintos sitios de las principales: Twitter, Facebook, XING y LinkedIn.
4. Arme una lista de los juegos educativos incluidos en las plataformas más utilizadas por sus hijos.
5. Identifique la información personal o confidencial que transmite online en servicios de e-mail y almacenamiento de datos y analice el riesgo de que esa información se pierda por completo.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

*04

Los peligros de Internet

La Red es un espacio común cuyo contenido y actividades son completamente dinámicos y están en continua evolución y cambio. Por esta razón, existen algunos riesgos inherentes a la estructura de Internet que se han convertido en puntos que se deben tener en cuenta a la hora de protegernos a nosotros mismos y a nuestras familias.

- Contenido inapropiado 70
- Descargas ilegales..... 73
- Ciberbullying..... 78
- Grooming 80
- Usurpación de identidad..... 84
- Malware..... 89
- Phishing 95
- Resumen..... 99
- Actividades..... 100



Contenido inapropiado

La gran vidriera de la Web se nos presenta de manera tan libre como si se tratara de un shopping o una galería de arte. Con solo colocar la dirección correcta en el navegador accedemos al sitio que proporciona el contenido. Ahora bien, dependiendo de la edad del usuario, ciertos contenidos podrían ser considerados **inapropiados**, como, por ejemplo, todo lo relacionado con la pornografía, la violencia y otros.

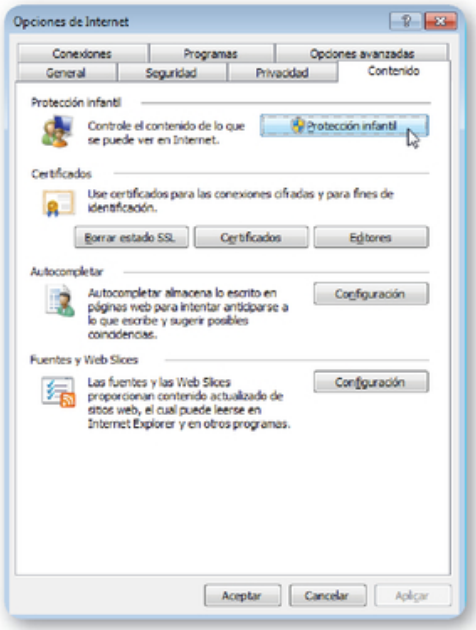


Figura 1. Windows cuenta con una opción para configurar de manera básica el control parental (también llamado **`Protección infantil`**), desde las opciones de Internet.

> EL CONTROL QUE IMPLEMENTAN LOS PADRES ESTÁ LIMITADO AL EQUIPO DEL HOGAR

Es **muy difícil garantizar** que si un menor quiere acceder a un contenido no lo hará finalmente, ya que los mecanismos de control y filtrado con que pueden contar los hogares están limitados a los sistemas y computadoras en los que se instalan y ejecutan. De esta manera, el menor podría contar con **otra computadora**, ya sea una conexión pública, el equipo de un amigo, conocido o de la escuela y así acceder a lo que quiera sin que los padres puedan tener control ni conocimiento de lo que el niño navega.

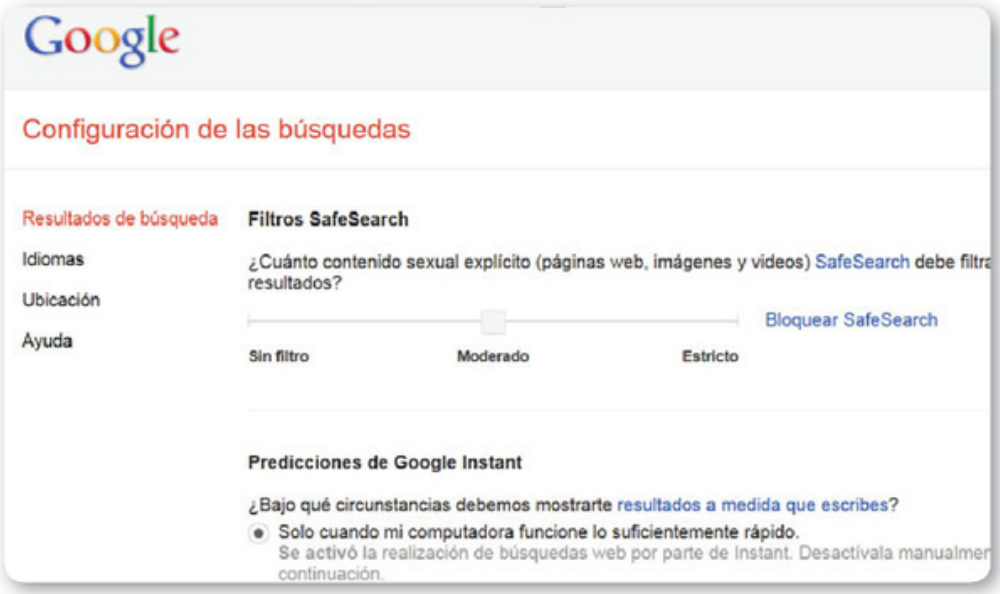


Figura 2. El filtro **SafeSearch** de Google permite definir el nivel de contenido adulto de los resultados de búsqueda.

El contenido inapropiado es, sin dudas, uno de los peligros más destacados en Internet, ya que forma parte de la estructura de la red y no es posible aislarlo con facilidad. No obstante, mantener los sistemas operativos **limpios** de código malicioso puede ayudar mucho a que no aparezcan **ventanas emergentes** y otros **carteles** embebidos en sitios web cuando se navega a diario.



Figura 3. **Zoodles** (**www.zoodles.com**) es uno de los programas más populares para control parental.

Otro modo de limitar la visualización de estos contenidos es mediante el software de **control parental**, cuyos mecanismos de filtrado pueden ayudar a seleccionar qué información será mostrada. Además, los motores de búsqueda como **Google** y **Bing** poseen opciones de configuración que brindan la posibilidad de no mostrar contenidos **exclusivos para adultos**.

En suma, los contenidos serán inapropiados dependiendo del perfil del menor, su **edad**, la sociedad en la que crece, sus padres, su **educación**, su **religión** y otras variables. Si bien los mayores siempre se han preocupado por **proteger a los niños** del material que pueda provocarles cualquier clase de perjuicio, el problema con Internet se multiplica por el hecho de que es muy difícil controlar todos los puntos de acceso y deben tomarse medidas generales que incluyan instrucciones a los menores sobre qué hacer en caso de que visualicen cosas que puedan considerar **extrañas**, **violentas** o **inadecuadas** para su edad.



Figura 4. **KidBox** (**www.kidbox.net**) es un conocido software de control parental con muchas opciones para regular la navegación de los menores.

La configuración de las opciones de control parental de los buscadores más conocidos es muy simple. En el caso de Google, basta con iniciar sesión, ir a **www.google.com/preferences** y ajustar la opción en **Moderado** o **Estricto**, como se indica en la **Figura 2**. La opción **Estricto** implica que se filtran el texto, las imágenes y los videos de contenido para adultos de los resultados de la búsqueda. En la

opción **Moderado** no se filtra el texto. Para el caso de Bing, también será necesario iniciar sesión para que el sitio pueda reconocer y recordar nuestras configuraciones personales, y luego ir a **www.bing.com/preferences.aspx** para acceder de forma directa. Una vez allí, debemos seleccionar la opción deseada (se utilizan los mismos nombres en ambos buscadores).

Descargas ilegales

Internet ha pasado de ser un espacio virtual con contenidos dispersos a un gran escenario con terabytes y terabytes de contenido ordenado y organizado para que sea fácil de encontrar. Con este panorama, se popularizaron con el tiempo los **sitios de descarga** de archivos que, luego de pasar por varias instancias tecnológicas, terminaron conformando una estructura basada en un sitio web con información cuidadosamente **indexada**, cuyos contenidos están almacenados en sitios llamados de **descarga directa** como el famoso **Rapidshare** y el discutido **Megaupload**, que fue cerrado por el **FBI** por ser acusado de alojar **material ilegal**. Lo cierto es que los sitios de descarga directa proveen acceso a archivos que son subidos por usuarios y no controlan sus contenidos específicos (ni es su función principal), de tal manera que si se suben archivos comprimidos y con clave, solo quienes los descargan y cuentan con la información necesaria podrán acceder a ellos.

> LOS SITIOS DE DESCARGA DIRECTA NO CONTROLAN EL CONTENIDO SUBIDO POR LOS USUARIOS

HERRAMIENTAS DE CONTROL PARENTAL

Son programas que permiten controlar el acceso a sitios web utilizando dos técnicas principales: el uso de **listas**, donde se detallan los sitos que se desea bloquear explícitamente (lista negra) o a los que es posible acceder (lista blanca); y la detección de **palabras clave**, para que el software compruebe el contenido de los sitios y deniegue el acceso a los que las incluyen.



Figura 5. **RapidShare** (**https://rapidshare.com**) es uno de los sitios más populares de descarga directa.

Antes, para alojar archivos debía utilizarse el propio servidor web u otro servicio de **hosting** que permitiera almacenar grandes volúmenes de información. Hoy en día, los sitios que prestan servicios de carga y descarga de archivos han cubierto esa necesidad sin que sea necesario gastar dinero en eso.

A primera vista, las descargas directas no parecerían acarrear ningún problema asociado, pero el inconveniente aparece porque al no estar validado el contenido de los archivos que se descargan, podría incluirse en ellos **música**, **películas**, **software** y cualquier tipo de información que requiera una **licencia** específica para su uso. La descarga de este tipo de productos es **ilegal** si no hemos adquirido la licencia de uso que corresponde en cada caso.

EL CASO MEGAUPLOAD

Megaupload, creado en 2005 por **Kim Dotcom Schmitz**, fue uno de los sitios de descarga directa más populares hasta 2012, cuando el FBI provocó su cierre y arrestó a varios de sus directivos en Estados Unidos y Nueva Zelanda. Como evolución y sucesión de Megaupload, se lanzó a principios de 2013 el sitio **Mega** (**https://mega.co.nz**), para continuar prestando servicios de almacenamiento en la nube.



Figura 6. **MediaFire** (**www.mediafire.com**) es otro sitio popular de almacenamiento de archivos para descarga directa.

Más allá de la ética de la descarga de contenidos licenciados, existen peligros asociados a la **posibilidad de infectarse** con algún tipo de **software malicioso** en el afán de obtener esos archivos, programas o contenidos multimedia.

> INSTALAR SOFTWARE USANDO CRACKS O PARCHES ES ILEGAL Y PUEDE INFECTAR NUESTRO SISTEMA

Sin saberlo, muchas personas se bajan software ilegal que instalan por medio de alguna especie de parche o **crack**, que es el mecanismo que ha creado algún **cracker** para desproteger el software original del fabricante. Si bien esto es algo ilegal en sí mismo, nuestro foco está puesto en el peligro de infectarnos y no en las consecuencias éticas y legales que puede traer este comportamiento.

NAPSTER, EL PIONERO

Napster, un programa creado en 1999 por **Sean Parker** y **Shawn Fanning**, fue el primer proyecto de descarga directa y estaba orientado exclusivamente al intercambio de música. El caso tomó relevancia internacional al manifestarse la ilegalidad de la descarga de estos contenidos, lo cual le valió denuncias de varias compañías discográficas. A mediados de 2001 fue cerrado y transformado con el tiempo a una versión paga.



Figura 7. Taringa! (**www.taringa.net**) es una popular comunidad virtual que ha sido foco de noticias en 2011 por facilitar el acceso a contenidos de terceras partes.

Asimismo, existen programas llamados de **P2P** (**Peer to Peer**) que utilizan protocolos homónimos para interconectarse y permitir que el lugar de alojamiento de los contenidos sean los propios equipos de los usuarios, promoviendo el intercambio de archivos **de a pares** de manera más personalizada, pero con los mismos riesgos mencionados antes. Ejemplos de programas P2P son **eMule**, **eDonkey**, **Kazaa**, **Ares**, **BitTorrent** y **Azureus**. El motor de búsqueda de archivos P2P más popular de la red fue **The Pirate Bay**, un sitio web sueco que llegó a centralizar la mitad del tráfico de este tipo del mundo. En 2008, sus dueños fueron acusados de violación a derechos de autor y condenados a prisión y al pago de una multa millonaria.

Muchas personas incluso desconocen que el software o la música deban adquirirse pagando una determinada suma de dinero, lo que se ve en especial en países de Latinoamérica y otros tantos en vías de desarrollo. La **cultura de lo gratuito** en este caso es una tremenda arma de doble filo, que comúnmente termina en la infección de equipos con consecuencias graves para la **privacidad** de sus usuarios. Por este motivo, debemos tener cuidado al descargar contenido de Internet, pues aunque parezca a veces muy simple y sencillo, puede esconder algunas problemas no tan evidentes.



Figura 8. Vuze (previamente Azureus) es un cliente de BitTorrent que permite descargar archivos de redes P2P.

Cuando se desee descargar algún software, siempre se recomienda hacerlo desde el **sitio del fabricante**, de manera tal de garantizar la integridad de la descarga y poder cerciorarse de que solo se está descargando lo que se deseaba bajar, sin posibles agregados maliciosos que puedan dañar nuestro equipo.



Figura 9. Luego del cierre de Megaupload, su creador lanzó Mega, un nuevo servicio de almacenamiento de archivos en la nube.

Ciberbullying

La **violencia infantil** y juvenil no es algo nuevo en las sociedades, sino que se ha mantenido en muchos sectores de la población a través de los tiempos. La diferencia hoy en día radica en el modo en que esta se manifiesta, lo que le ha dado masividad hasta ocupar incluso las primeras planas de periódicos y otros **espacios importantes** de los medios masivos de comunicación. Si bien esta difusión masiva ha alcanzado en gran medida a los padres y docentes y ha llevado el tema a las mesas de trabajo de centros educativos, muchas sociedades menos beneficiadas económicamente no han podido ser alcanzadas por las **medidas paliativas recomendadas** porque en algunos sectores la educación no ocupa un lugar central debido a la existencia de **problemas más radicales**, como la pobreza, la falta de salud y el hambre, todas íntimamente relacionadas.

Entre las prácticas que muchas personas han padecido, en especial en la etapa escolar, se encuentra el llamado **bullying**, que es el nombre que se le dio en los países angloparlantes al comportamiento basado en el **acoso de un menor a otro** o de un mayor a un menor. Los medios de acoso tradicionales incluían las vías de contacto comunes, como el teléfono, los mensajes escritos y el diálogo oral directo.



Figura 10. Muchas discusiones entre los adolescentes pasan al ámbito virtual y pueden derivar en ciberbullying.

Con el advenimiento de los medios de comunicaciones digitales e Internet, estas prácticas se extendieron y derivaron en lo que hoy conocemos como **ciberbullying**, es decir, una ampliación de las vías del acoso tradicional hacia los canales modernos de contacto.

PROBLEMAS RADICALES

Aplicando el modelo de la pirámide de necesidades de **Abraham Maslow** a las necesidades sociales, tendríamos en la base las necesidades básicas, un segundo nivel incluiría la educación y el desarrollo, y en un tercero se encontrarían el entretenimiento, la conciencia social, la libertad financiera y la trascendencia de lo personal. Cada nivel está menos relacionado con la supervivencia que el anterior.



Figura 11. **StopBullying** (**http://espanol.stopbullying.gov**) es un sitio del Gobierno estadounidense con mucha información sobre ciberbullying, disponible en español.

Esta conducta incluye el **chantaje**, **insultos**, **injurias** y **agravios** de una parte hacia su víctima, y supone normalmente el uso de información difamatoria difundida por medios electrónicos, como mensajes de texto, correo electrónico, mensajería instantánea, redes sociales y demás. También puede incluir la publicación de videos, fotografías o cualquier tipo de material que permita ejercer **violencia emocional y psicológica**. Así, suelen proliferar páginas de **Facebook** o blogs destinados a **odiar a una persona** cuya intención es desconocida por la red social o servicio de blogs y, por lo tanto, hasta que el sitio no reciba una denuncia, su continuidad ni siquiera será evaluada.

Este comportamiento que se ha dado por décadas en las escuelas solía **finalizar con el tiempo**, cuando el agresor encontraba otro motivo de diversión, otra vía para canalizar su violencia o cuando desaparecía la gracia que le pudiera producir tal accionar. En el caso de su versión digital, el problema es mayor ya que la publicación de un contenido en Internet hace que **el asunto no finalice**, sino que las pruebas visibles quedan online por **tiempo indeterminado**, incluso cuando el acosador haya dejado de atentar contra la salud emocional de su víctima, ya sea por pérdida de interés o cualquier otro motivo.



Figura 12. `CiberBullying.com` es un proyecto de la iniciativa `Pantallas Amigas` para la lucha contra el ciberbullying.

Diferentes proyectos de investigación han permitido delimitar algunas de las **características distintivas** o hasta verdaderos perfiles psicosociales de las víctimas y de los agresores, lo que en cierto modo nos aproxima cada vez más a las alternativas de solución. De cualquier manera, todas las formas de abuso que se encuentran potenciadas por los nuevos canales de comunicación no son más que una **manifestación de un problema subyacente**, que debe ser abordado desde su génesis profunda para poder ser prevenido como riesgo social emergente.

Grooming

En términos sociológicos, podemos definir el **grooming** como el **engaño de una persona adulta a un menor** de edad a través de los diferentes medios de contacto que son utilizados normalmente para comunicarse entre la gente. En general, el objetivo de este tipo de engaños es la obtención de **imágenes de contenido sexual** del menor que después el acosador utilizará para ejercer **coacción** y **extorsión** sobre el menor. Básicamente, esto es **una clase de abuso sexual** solo que es desarrollado de manera virtual, con el objetivo de obtener material comprometido en términos sexuales por medio de una

relación de **sometimiento** del adulto hacia el menor. Esta relación pasa del engaño a la extorsión, bajo la **amenaza** de publicación del material obtenido, **difusión** de la información o **divulgación** a amigos y familiares. En el más avanzado de los casos, el agresor busca concretar un **encuentro presencial** para materializar el abuso sexual.



Figura 13. **QueNoTeLaDen** (**www.quenoteladen.es**) es una importante iniciativa española de lucha contra el grooming.

El grooming suele transcurrir a lo largo de una serie de fases relativamente constantes y continuas que permiten establecer un esquema para estudiarlo, investigarlo y reconocerlo. Las distintas fases que atraviesa son las siguientes:

- **Fase inicial o de amistad**: el adulto **simula ser un niño** o un joven de edad cercana a la del menor e intenta establecer lazos de



RIESGO SOCIAL

Ciertas prácticas introducen lo que se denomina **riesgo social**, que en términos simples es la probabilidad de ocurrencia de un peligro social. Ese peligro es aquello que puede afectar de manera negativa a los distintos componentes de una sociedad, comenzando por la familia. Tanto el **cyberbullying** como el **grooming** están considerados como prácticas generadoras de riesgo social.

confianza o compromiso mediante la búsqueda de **elementos en común**, como los gustos, preferencias y cualquier otro aspecto que pueda representar coincidencias que, aunque falsas, atraerán al menor. La fase es neutra desde el punto de vista de la violencia o los diálogos lascivos. El menor **no sospecha** de su interlocutor.

- **Fase de relación**: el adulto va obteniendo **datos personales**, familiares, sociales, de contacto del menor, de toda su familia, grupo de amigos y relaciones. En esta etapa comienza el intercambio de confidencias, secretos y conversaciones íntimas encaminadas a **ganarse el afecto** del menor, despertar en él admiración, pena o compasión. Se busca generar algún tipo de **dependencia emocional** que el menor confunda con entendimiento, empatía o amistad para que no le permita desplegar mecanismos de defensa.
- **Fase de actuación**: una vez ganada la **confianza** y satisfechas todas las demandas iniciales, se pasa a la obtención de imágenes comprometidas, expresiones, sonidos y actos de naturaleza sexual explícita, utilizando principalmente una **cámara web** o un **teléfono celular** para obtener este material.



Figura 14. **Trust** es una película protagonizada por Clive Owen donde se representa el sufrimiento de las víctimas de grooming y de sus padres.

EL CASO AMANDA TODD

En octubre de 2012, Amanda Todd, una adolescente canadiense de 15 años, se suicidó tras haber sido víctima de grooming y bullying durante más tiempo del que pudo soportar. Lo que hizo que el caso tomara relevancia fue que ella dejó un video grabado, contando su historia, que resultó en un testimonio desgarrador que sienta precedentes sobre la importancia del acoso virtual.

El proceso general suele durar desde varios días hasta semanas o meses. Normalmente, **se inicia por medio de redes sociales** o medios que parezcan más inocentes y luego, se pasa a vías de contacto más directo como la mensajería instantánea. En muchos casos, el agresor **logra obtener la contraseña** de la cuenta de correo electrónico, red social o sistema de mensajería instantánea del menor, y se lo hace saber para comenzar la **manipulación directa** y el chantaje, que deriva en pedidos amenazantes de los que el menor ya no puede escapar.

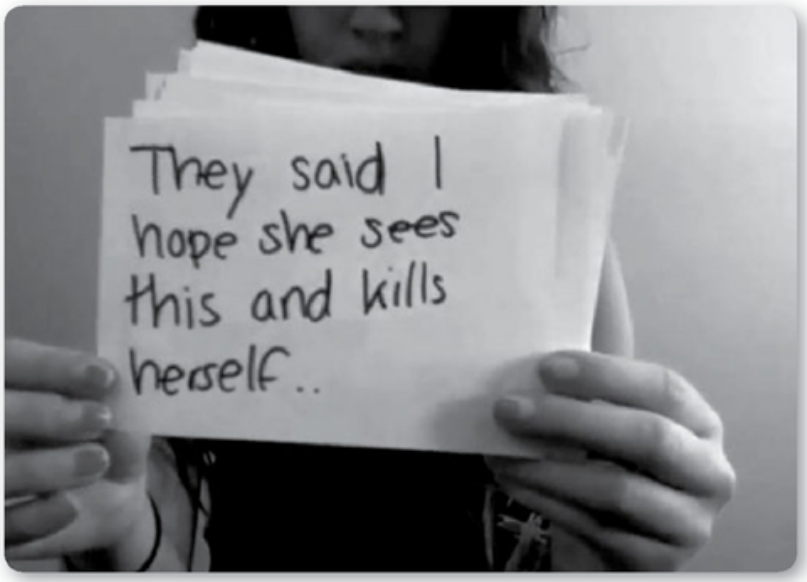


Figura 15. Imagen del video que dejó Amanda Todd antes de suicidarse, víctima de acoso y extorsión.

Lamentablemente, cuando los menores logran detectar la peligrosidad de estos agresores **suele ser tarde**, pues ya se encuentran envueltos en la **perversión de su juego**. No obstante,

TENDENCIA CRECIENTE

Resulta de extrema complejidad relevar a ciencia cierta los casos de bullying y grooming, aunque las cifras ya marcan una **tendencia en crecimiento** que permanece opacada porque las víctimas no suelen contar su situación, en general, **por miedo**, produciendo un sufrimiento silencioso que puede afectar el **desarrollo emocional** del niño, dejando **secuelas** permanentes a nivel psíquico y físico.

cualquier adulto podría identificarlos en base a los elementos básicos de su **conducta**, como, por ejemplo, la complejidad de las preguntas que realiza, su uso del lenguaje o la tendencia de sus intenciones. Es posible reducir el riesgo si al menos los primeros contactos que tenga el menor en redes sociales y por otras vías de comunicación son **supervisados por un adulto**.

Usurpación de identidad

La usurpación o robo de identidad es, en la actualidad, el delito de más **rápido crecimiento** en el mundo, y se relaciona con el robo de datos personales para ser utilizados de manera fraudulenta, como el número de documento, **tarjeta de crédito o débito** y otros. A esto se le suma la posibilidad de obtener otros datos vía Internet en base a perfiles de redes sociales y demás.

Un usurpador de identidad busca realizar actividades en nombre de otra persona, tanto **física** como **virtualmente**. En general, la víctima **no se entera** de que ha padecido tal robo hasta que, por ejemplo, le niegan un crédito o la contratación de un servicio, ve operaciones sospechosas en sus resúmenes de tarjetas de crédito o bien, al querer registrar un perfil online, descubre que ya está siendo utilizado.

Este problema también se encuentra relacionado con los **menores** de la familia en el punto en el que ellos conocen información personal de sus padres y podrían facilitarlos a potenciales delincuentes de manera directa o indirecta. Además, muchas veces los niños, sin poder tomar conciencia del riesgo, brindan **información sobre la familia**, los bienes, las actividades y otros datos de alta sensibilidad. Por esto,

EN LOS CAJEROS AUTOMÁTICOS

Siempre se recomienda utilizar para abrir la puerta una tarjeta distinta a la utilizada para operar. De esta manera, no podrá relacionarse la banda magnética con el PIN si es que se han colocado dispositivos de **sobrelectura** o **sobreteclado**. En muchos países es común el uso de **pescadores**, elementos que retienen el dinero para evitar que salga físicamente, a pesar de que la operación fue correcta.

si bien el robo de identidad está asociado por obvias razones a los mayores de edad, los menores podrían formar parte del problema cuando son usados como canal.

Un estafador buscará **efectuar gastos** con tarjetas robadas, abrir cuentas para emitir cheques, obtener préstamos o acceder a servicios de **trámites rápidos** (sin demasiadas comprobaciones), como los de telefonía celular o créditos a sola firma. Si hay dinero en las cuentas, el delincuente lo extraerá por **cajero automático**, ventanilla o de manera virtual en caso de que haya obtenido sus datos de usuario y contraseña de **homebanking**. Otras estafas incluyen la producción de documentos de identidad falsos **a nombre de la víctima** pero con la fotografía del impostor para conseguir empleo o cometer otros delitos y responder con tal identidad a las demandas, lo que provocaría citaciones a la persona real. La ventaja del estafador es que prácticamente todo trámite que incluya datos personales puede dejar huellas, y hasta los propios **residuos personales** pueden contener información sensible.



Figura 16. Cuidar nuestras transacciones bancarias por cajero automático ayuda a reducir el riesgo de robo de identidad.

Es recomendable **evitar llenar formularios** o **encuestas** en la vía pública y tener cuidado con los petitorios que, simulando una causa noble, se pueden utilizar para recabar datos de la gente.

Muchas acciones cotidianas **dejan huellas** tanto virtuales como físicas, desde el acceso al e-mail o a las estaciones de trabajo, el ingreso físico a

edificios y oficinas, hasta los molinetes automáticos de los subterráneos, las máquinas de transportes públicos, las puertas de cajeros automáticos.

Por todo esto, es recomendable llevar encima solo las tarjetas y la **documentación necesaria** y minimizar los papeles importantes que cargamos, como partidas de nacimiento, certificados y pasaportes. De hecho, podríamos evitar el uso del documento de identidad salvo que sea estrictamente necesario, aunque de todas maneras el número de documento no es considerado un **dato sensible** a nivel legal ya que puede obtenerse de padrones electorales, organismos públicos o entidades de recaudación fiscal.



Figura 17. Contrastar los resúmenes de tarjetas de crédito con los tickets y facturas ayuda a detectar el fraude y el robo de identidad.

También se sugiere recortar las tarjetas vencidas antes de tirarlas en un lugar seguro y cerrar las cuentas bancarias inactivas. Para los PIN de las tarjetas, es mejor prescindir de los **datos numéricos personales** (teléfono, DNI, fecha de nacimiento, etcétera). Podemos aprovechar la metodología de contraseñas visuales, que se recuerdan por la ubicación en el teclado en lugar de la combinación de caracteres. Aunque es difícil de creer, muchos usuarios escriben su PIN en la tarjeta para no olvidarlo.

En caso de que haya personas trabajando en nuestra casa, es aconsejable mantener la información personal en un **lugar seguro** o apartado, y cuidarnos también de la sustracción de cartas y sobres que llegan al **buzón de correo postal**.

Es bueno conocer la **política de privacidad** de las entidades bancarias antes de operar con ellas, para saber cómo podrán disponer de nuestra información personal. También es recomendable pedir un **informe crediticio** por lo menos una vez al año para revisar si nos aparece alguna actividad fraudulenta o sospechosa.

Es importante conservar la documentación y los registros de las **transacciones electrónicas** y no enviar información financiera por correo electrónico, salvo que usemos algún **sistema de cifrado de mensajes**.



Figura 18. El sitio Identidad Robada (`www.identidadrobada.com`) es fuente de referencia obligada en español sobre el robo de identidad.

Si hemos sufrido el robo de identidad, debemos **tomar medidas de manera inmediata** y mantener un registro de todas las llamadas telefónicas y otros tipos de contacto con empresas en relación al fraude. El primer paso será realizar **denuncias**, principalmente a la

MENSAJES DE CORREO CIFRADOS

Para el envío de correo electrónico de manera segura existen distintas opciones y software de cifrado, que permiten encriptar los mensajes enviados para que solo puedan ser vistos por el emisor y el receptor. **PGP** (**Pretty Good Privacy**) es uno de los sistemas más utilizados para realizar estas operaciones, que suelen hacerse solo entre usuarios de amplios conocimientos técnicos. Su versión libre se denomina **GPG** (**GNU Privacy Guard**).

policía local, las empresas con las que realizamos transacciones y los bancos con los que operamos. En cuanto a la denuncia policial, debemos conservar el certificado a fin de tener **constancia del delito** y poder demostrar inocencia si en el futuro aparecen operaciones o acciones en nuestro nombre. También debemos **suspender las tarjetas** y avisar a las compañías de informes crediticios.

Hay que tener en cuenta que, por lo general, las leyes **no brindan suficiente protección** cuando se ha producido un robo de identidad ni permiten realizar cambios en el número de documento, aunque sí a veces en el nombre y el apellido.

En los casos de robo de número de tarjeta de crédito y PIN, las operaciones fraudulentas pueden ser hechas tanto en tiendas físicas como virtuales. Debe comunicarse la situación de inmediato al banco emisor o a la empresa de tarjetas en cuestión. Las **transacciones online** y las compras virtuales **suelen ser muy seguras**, el riesgo principal se encuentra normalmente en la inseguridad del sistema del usuario o en la imprudencia en su uso.

Para el caso del robo de **identidad virtual**, los sitios de redes sociales y foros suelen tener algún mecanismo de denuncia que permite **recuperar** lo perfiles robados o usurpados. Aunque esta utilidad funciona relativamente bien, siempre es más fácil prevenirse mediante el uso prudente.



Figura 19. Facebook proporciona un canal de denuncias para el caso de que nuestro perfil haya sido usurpado o falsificado.

Malware

Se llama **malware** (**malicious software**) a todo tipo de código malicioso. Si bien se cree muchas veces que se trata solo de **virus**, esto no es así en la actualidad, ya que estos últimos apenas representan un pequeño porcentaje de todo el malware existente.

Un malware no es más que una pieza de software diseñada para **infectar** un sistema con el objeto de concretar alguna acción maliciosa, intentando todo el tiempo evitar que el usuario **sospeche** de su presencia para que no intente eliminarla.

Su peligrosidad se establece en base a dos criterios principales: su capacidad de hacer **daño** y su posibilidad de **propagación**, y suele acarrear distintos tipos de problemas, principalmente relacionados con la **violación a la privacidad**.

Vale aclarar que no es posible producir daños físicos permanentes al **hardware** por medio de una infección a través de malware.

El ciclo de vida de esta clase de software es análogo al de los virus biológicos: **descubrimiento**, **propagación**, **infección**, **detección** y **erradicación**. La motivación principal para su creación es de tipo económica, para contribuir con el **cibercrimen** y el **fraude online** a nivel global, y no existe participación de las empresas antivirus, tal como se suele creer popularmente.

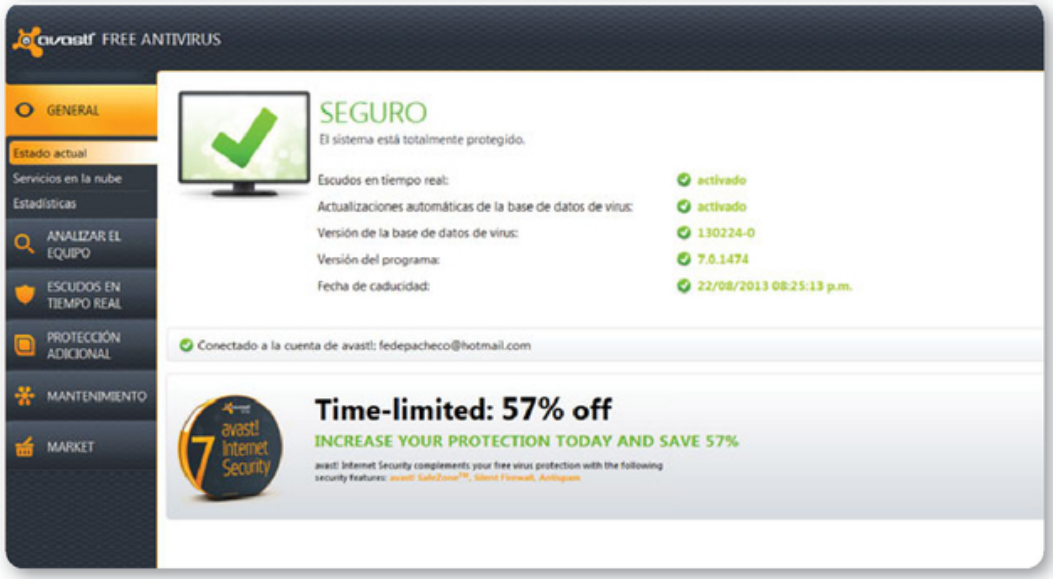


Figura 20. Avast! es uno de los antivirus gratuitos más utilizados (**www.avast.com**).

El malware puede clasificarse en función de **múltiples criterios** y un mismo tipo puede pertenecer a varias categorías. La clasificación principal, tomando en cuenta la forma en que se propagan, incluye: **troyanos**, **gusanos**, **adware, spyware** y **virus** propiamente dichos. Cabe destacar en particular el comportamiento de los gusanos, que no necesitan infectar otros archivos para multiplicarse ya que aprovechan **vulnerabilidades de los sistemas** y aplicaciones para su propagación, por lo que se recomienda siempre mantener los sistemas operativos y aplicaciones actualizados.

Tomando en cuenta sus acciones pueden encontrarse **keyloggers**, **backdoors**, **ransomware**, **rogue** y **rootkits**. Como nuestro objetivo no es ahondar en conceptos técnicos, solo describiremos las categorías principales o las funciones para reconocer el malware.



Figura 21. AVG es otro famoso programa antivirus con versión gratuita (**`http://free.avg.com`**).

ANTIVIRUS GRATUITOS: ¿SÍ O NO?

Si bien los productos antivirus suelen ser pagos, muchos cuentan con versiones gratuitas o de uso personal. En términos generales, es mejor utilizar un antivirus gratuito original que un antivirus **crackeado** o con licencia falsa, ya que estaríamos poniendo nuestra seguridad en manos de usuarios desconocidos relacionados con la piratería de software.

Si bien las principales medidas de protección pasan por el uso de un **software antivirus**, es necesario utilizar Internet y las computadoras con prudencia para evitar las infecciones. Pese a que la mayoría de las veces que nos referimos a malware estamos hablando sin decirlo de los sistemas **Windows**, también existen **códigos maliciosos** que afectan a otras plataformas, como **Linux** y **Mac**. Si bien esto puede parecer a primera vista imposible, solo basta decir que gran parte de las infecciones están vinculadas al **comportamiento del usuario** y no del sistema operativo, y el hecho de que nuevos sistemas estén disponibles para usuarios finales hace que se desarrollen códigos maliciosos para aprovecharse de ellos.



Figura 22. Muchas empresas de antivirus ofrecen herramientas específicas gratuitas como esta de **Kaspersky** para remover **Flashback**, un troyano para Mac OS.

Existen aplicaciones específicas llamadas **keyloggers**, que tienen la capacidad de grabar todo lo escrito por el teclado para luego enviarlo a otro lugar o almacenarlo a la espera de ser recuperado. Si bien su principal implementación es en software, existen **dispositivos de hardware** que ofrecen las mismas funcionalidades: se colocan a modo de adaptador entre el cable del teclado y el conector del **motherboard** y almacenan la información en una **memoria interna**.

Dado su origen como herramienta espía, una de sus características es pasar desapercibido al momento de la instalación, uso y reporte.

Muchas veces son utilizados en empresas para vigilar empleados o en hogares para **vigilar a los menores**. De hecho, una de sus utilidades es que pueden ser configurados para alertar al momento de interceptar ciertas **palabras clave**.

Aunque existen algunos programas detectores de keyloggers, un antivirus se considera en sí una contramedida aceptable en el caso de no estar siendo utilizados deliberadamente para vigilancia.

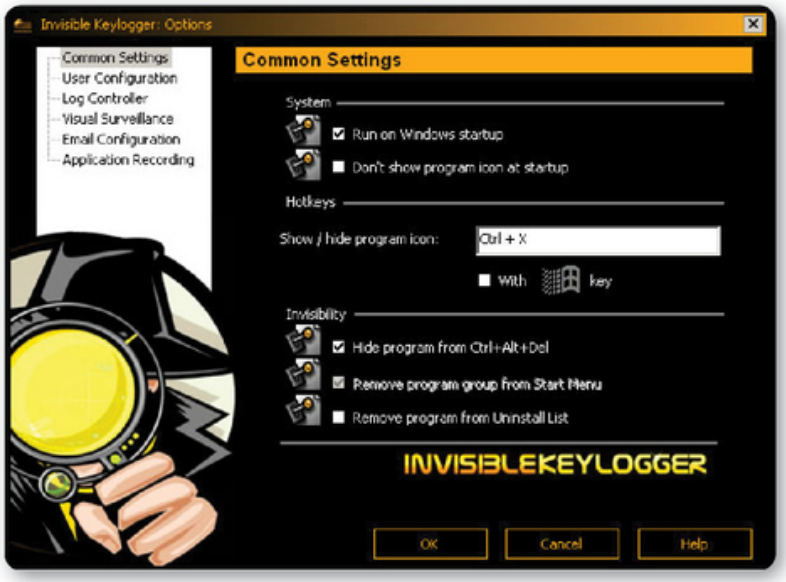


Figura 23. Algunos padres prefieren monitorear a los niños con herramientas avanzadas como los keyloggers. Aquí, la pantalla de **`Perfect Keylogger`**.

Otro tipo de malware peligroso son los troyanos, que llevan **oculta una funcionalidad** que será usada con fines maliciosos contra el usuario que lo ejecuta. La idea está tomada de la mitología griega, refiriéndose al **caballo de Troya** recibido como regalo de buena fe y en cuyo interior se escondían soldados enemigos.



MALWARE EN CELULARES

Los códigos maliciosos alcanzan también a las plataformas móviles y **smartphones**, como **iPhone**, **BlackBerry** y equipos con **Android**. El malware para celulares se está extendiendo cada vez más, basado en el aprovechamiento de las imprudencias y el desconocimiento de los usuarios de telefonía celular. Por supuesto que también existen programas antivirus para estos dispositivos.

Una de las principales diferencias entre un **virus** y un troyano es la inhabilidad de este último para replicarse. Si bien no necesariamente debe funcionar como **puerta trasera** de acceso a un sistema, la mayoría de ellos lo hace, y por lo tanto se ha de tener en cuenta su aplicación como herramienta de **administración remota** subrepticia. En base a esta característica es que existen programas especiales con estas funcionalidades y otras adicionales para ser utilizados como mecanismos de vigilancia y control parental.

Los troyanos suelen llegar al sistema como programas **en apariencia inofensivos**, que pretenden ser algo que no son o hacer algo que no hacen. A veces, se envían como **adjuntos de correo** fingiendo ser una utilidad de sistema, otras veces llegan como parte de una aplicación **troyanizada**. De hecho, mucho malware posee la capacidad de introducir y ejecutar troyanos y keyloggers como parte de su accionar malicioso. Algunas características comunes de los troyanos son la edición del registro, apagado o reinicio del sistema, robo de contraseñas, captura de pantallas, grabación de teclas, monitoreo del tráfico, ejecución de aplicaciones y manipulación de archivos.



Figura 24. The Cleaner nació como producto específico para combatir los troyanos, hoy limpia además todo tipo de malware.

Otra categoría destacable es el **spyware**. Su historia comienza con la introducción del **Adware** (**Advertising Supported Software**), que implica la introducción de publicidad en el software para que los

programadores puedan recibir dinero de las empresas que allí publicitan y así poder continuar manteniendo los programas en modo gratuito (**freeware**). Con el tiempo, esta idea se tergiversó y derivó en el concepto de **spyware** (software espía), un tipo de malware que afecta de manera directa la privacidad, recopilando información de personas y organizaciones sin su consentimiento, con fines comerciales. Esta cadena está formada por programadores que incluyen spyware en sus aplicaciones a cambio de dinero, empresas dedicadas a la implementación de productos de medición de audiencia y empresas de marketing y publicidad que procesan la información y brindan servicios como estudios de mercado, penetración de productos, perfil del consumidor, información demográfica, etcétera. Muchos productos cuestionados por incluir spyware suelen advertir de manera **explícita** sobre su accionar en sus licencias, que casi nadie se detiene a leer.

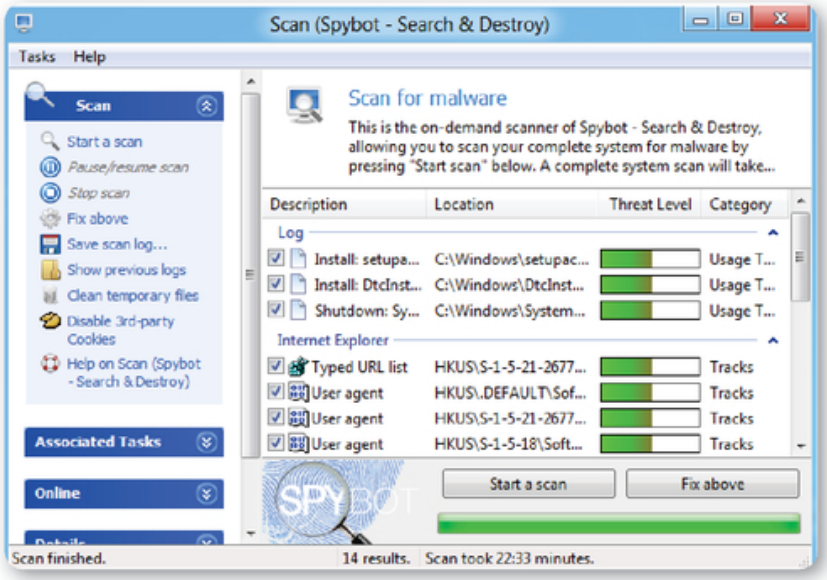


Figura 25. Existen productos específicos para combatir el spyware, como Spybot (**www.safer-networking.org**).

CÓMO FUNCIONA UN ANTIVIRUS

Un antivirus tiene un módulo de **control** y uno de **respuesta**. Realiza la detección usando **firmas** para comparar patrones estáticos y **heurística**, que se basa en el análisis de **comportamiento**. Intenta limpiar el sistema infectado y si no puede, guarda la amenaza para analizarla con futuras actualizaciones (**cuarentena**).

La última categoría corresponde a los llamados **rogue** o software falso, que pueden llegar como **falso antivirus** o herramienta de limpieza del sistema o cualquier otra utilidad que simule realizar funciones importantes. Estos programas no tienen necesariamente un comportamiento malicioso sino que llevan al usuario por medio del engaño a **registrarse** y pagar una pequeña suma de dinero por una versión completa del programa, que se supone le permitirá reparar o limpiar su sistema. Cuando este accede, se encuentra con carteles y avisos de que todo está bien y ha sido arreglado, pese a que nunca se ha tenido ningún problema real. Para prevenirse de esta amenaza, es fundamental evitar descargar software que no provenga de empresas confiables y marcas reconocidas.

Phishing

El **phishing** es una técnica que implica el **engaño** a los usuarios con el fin de intentar obtener información personal, como contraseñas, cuentas bancarias, datos de tarjetas de crédito, etcétera. Como podemos imaginar, esto se realiza en forma **fraudulenta**. El **modus operandi** del **phisher** incluye hacerse pasar por una persona o entidad de confianza y enviar un correo electrónico, un **SMS** o un contacto por mensajería instantánea, **imitando** el formato, el lenguaje e imagen de entidades bancarias o financieras, o bien del servicio con el que se desea engañar al usuario. La comunicación simula ser oficial y suele pedir algún tipo de dato de acceso o información relevante, alegando **motivos diversos** como la verificación de movimientos en el caso de cuentas bancarias, el cambio de políticas, evitar un posible fraude, etcétera.



LA PESCA DE DATOS

El término **phishing** deriva de la palabra **fishing** (**pesca**) y hace referencia al hecho de **pescar** contraseñas e información de los usuarios. La primera mención data de 1996 en un grupo de noticias de hackers, aunque apareció en la edición impresa del boletín 2600 Magazine y luego fue adoptado por crackers.

De esta manera, el phisher desea que la persona haga clic en un **link** a una página web **en apariencia real** pero que conduce a **sitios falsos** que simulan ser la página original con el objetivo de robar los datos ingresados. Dado que los usuarios pueden ver la página y tienen confianza en la entidad, suelen ingresar sus datos con normalidad. En caso de éxito, el phisher contará con información con la que puede realizar **compras por Internet** utilizando las cuentas o tarjetas de crédito, efectuar transferencias bancarias no autorizadas y otras operaciones. Además, el usuario suele perder el acceso a su cuenta, por lo que debe pedir su **recuperación** al sitio o institución.

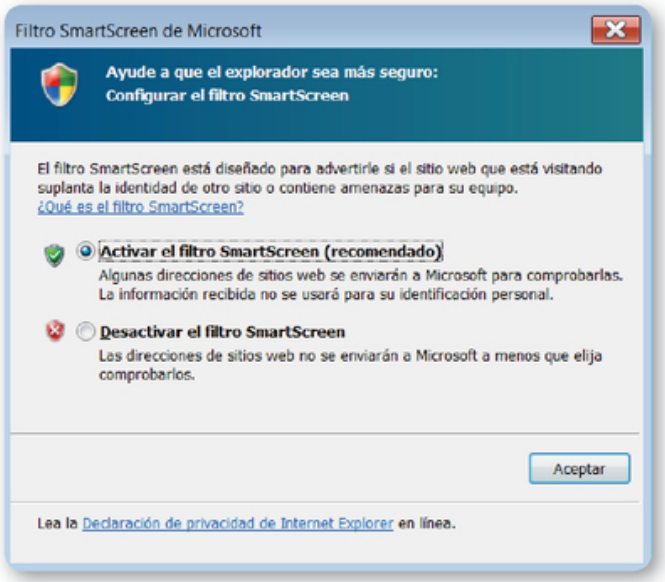


Figura 26. El filtro **SmartScreen** de Internet Explorer nos advierte cuando estamos por acceder a un sitio dudoso.

Otro tipo de phishing no bancario es el que promueven los sitios que proclaman identificar y mostrar los **contactos no admitidos**

¿CUÁL ES EL MEJOR ANTIVIRUS?

No es sencillo responder cuál es el mejor producto, pero hay varios laboratorios independientes que realizan pruebas comparativas y emiten informes públicos de sus resultados, detallando el tipo de análisis realizado. Los más importantes son: AV Comparatives (**www.av-comparatives.org**) y Virus Bulletin (**www.virusbtn.com**).

y eliminados de la lista de un determinado sistema de mensajería instantánea. Su único fin es robar los datos de usuario y la contraseña a cambio de mostrar algunos datos en general triviales que podrían obtenerse sin este **servicio**. Luego, con estos datos, podrían intentarse acceder a otros servicios relacionados, comunicarse con los contactos de la víctima, utilizar la cuenta para envío de **spam**, etcétera.

Para el caso específico de los menores, no consideramos el riesgo asociado al homebanking sino a cualquier otro sitio en el que tengan cuenta, como foros, sitios de juegos online, redes sociales y demás. Las técnicas utilizadas para el engaño en esos casos son las mismas que en el caso de los sitios de **banca electrónica**.

No existen métodos infalibles para detectar este tipo de ataques, por lo que la acción más relevante es **concientizar** a las personas sobre cómo reaccionar. Por ejemplo, si un usuario es contactado para verificar datos o cuentas, un comportamiento adecuado sería comunicarse con la institución que en teoría ha enviando el e-mail o ingresar en la barra de direcciones la Web que se reconoce como segura en lugar de hacer clic en el enlace del correo enviado. En el caso de menores, se los debe motivar a que ante la duda les pregunten a sus padres o a alguien que conozca del tema antes de tomar acciones o ingresar a sitios dudosos.

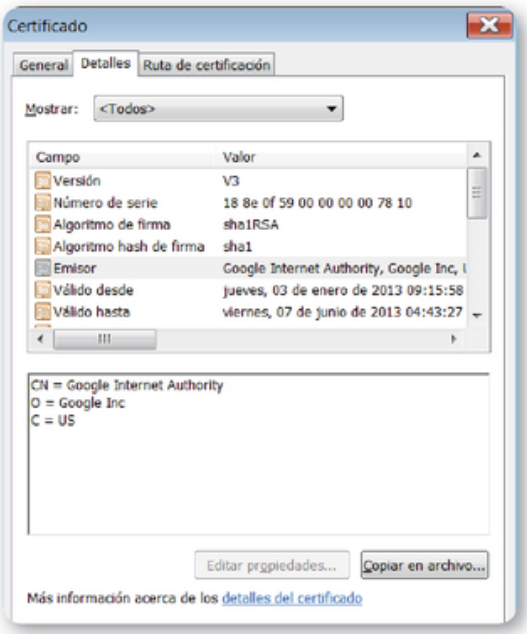


Figura 27. Los certificados digitales permiten comprobar la validez de un sitio. Aquí vemos el de Google desde Chrome.

El **Anti-Phishing Working Group** (**www.apwg.org**), asociación pionera y número uno en el tema, sostiene que al utilizar como componente principal la **ingeniería social** (técnicas de engaño que no se basan en la tecnología), las técnicas de phishing podrían quedar obsoletas en poco tiempo si se concientiza de manera correcta a los usuarios.

Otras respuestas son de índole técnica, con software **antiphishing** que puede complementar al antivirus y **firewall personal** o bien integrarse al navegador y trabajar identificando posible contenido fraudulento en sitios web o e-mails, utilizando listas de **URLs** reconocidas como maliciosas. A nivel corporativo, existen empresas y entidades que se dedican a monitorear y analizar continuamente los contenidos de compañías susceptibles de ser atacadas (bancos, entidades financieras, empresas de **e-commerce**, etcétera).

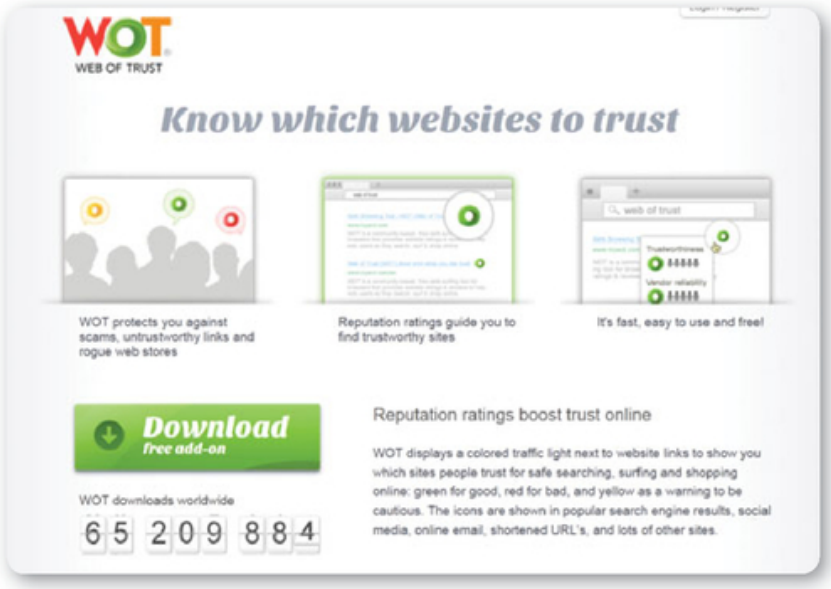


Figura 28. **WOT** (**Web Of Trust**) es un plugin para navegadores que permite obtener información de la reputación de los sitios web.

En general, se recomienda sospechar de cualquier e-mail que solicite información personal urgente y utilice argumentos como la mención de problemas técnicos, cambios de políticas de seguridad, promociones, premios, regalos, etcétera. También se sugiere no dejarse intimidar por los mensajes que advierten que si no se verifican o actualizan datos en un determinado tiempo se **cancelarán** o **bloquearán** la cuenta bancaria o el servicio al que se estén refiriendo, técnica que busca forzar a que el usuario responda

de inmediato. Desde luego que si no se es cliente de la institución de la que llega el mensaje, no quedan dudas de que es un engaño.

Una manera de verificar si el mensaje es fraudulento es notar que **no está personalizado**, aunque las técnicas modernas pueden inferir algunos datos específicos y simular un contacto especial.

Bajo el mismo parámetro de concientización, debemos evitar llenar formularios en correos electrónicos y sitios web no confiables y también evitar seguir links incluidos en los mensajes de correo. De manera lógica, antes de ingresar cualquier tipo de dato confidencial tenemos que asegurarnos de que nos encontremos en un **sitio seguro**. Para ello, debemos estar conectados a él mediante el protocolo **https** (aunque este protocolo en sí no implica total certeza sobre la identidad del servidor) y comprobar la veracidad de su **certificado digital**, accediendo a los detalles que ofrece cada navegador para ver la entidad certificante, su titular y su validez.

Los navegadores modernos poseen un **filtro** básico contra el phishing que se basa, por lo general, en el chequeo de **listas negras** y solo está pensado para actuar como primera línea de defensa. Nunca está de más revisar de manera periódica las cuentas bancarias para comprobar el estado de los movimientos o transacciones y, en caso de que haya alguno que no sea legítimo, denunciarlo en forma inmediata.

RESUMEN

En este capítulo hemos conocido los detalles de algunos de los riesgos más importantes a los que se está expuesto por el solo hecho de realizar actividades online, donde los menores se encuentran a veces muy desprotegidos. Analizamos la importancia de los contenidos inapropiados e ilegales y su vinculación con el malware, la necesidad de proteger la propia identidad digital para evitar su robo o usurpación y el phishing como técnica de engaño de los ciberdelincuentes. Además, explicamos dos peligros que introducen los riesgos sociales más grandes en lo relacionado con las tecnologías de la información, que son el grooming y el ciberbullying, temas que ningún padre o educador debería dejar de conocer.

Actividades

TEST DE AUTOEVALUACIÓN

1. Descargue un programa de control parental y analice en detalle sus funcionalidades.
2. Compare la cantidad de transacciones de dinero online que hizo en los últimos seis meses y las que hizo de manera física.
3. Verifique el software antivirus que tiene instalado en cada una de las computadoras del hogar y asegúrese de que está correctamente actualizado.
4. Motive a los niños a perder el miedo a contar los problemas que tienen en Internet con otras personas.
5. Averigüe en el colegio, el club y otros ambientes que frecuenten los niños si se han dado casos de bullying o ciberbullying, y si al caso se le dio el tratamiento adecuado. Luego, comparta las experiencias con otros padres y educadores.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

*05

El hogar moderno

En el presente capítulo veremos algunos temas asociados al entorno familiar y su relación con distintas tecnologías, como los teléfonos celulares, laptops y tablet PCs, y ofreceremos consejos para los mayores en cuanto al tratamiento de estos tópicos para con los niños.

- La familia y la tecnología 102
- El protagonismo de la PC..... 105
- Celulares y smartphones 108
- Los límites posibles 112
- Consejos para padres..... 114
- Consejos para menores 119
- Resumen..... 123
- Actividades..... 124

La familia y la tecnología

Bien es sabido que la familia es la más básica de las **estructuras sociales** y que en su seno se gestan los aprendizajes más profundos y valiosos de la vida, incluyendo los **valores**.

En ese contexto es que se aprenden las conductas que después se llevarán a los demás entornos, por lo que siempre se mantiene reflejado lo aprendido ahí.



En el hogar moderno se pueden encontrar muchos dispositivos tecnológicos, como teléfonos celulares, computadoras de escritorio, notebooks, **tablet PCs**, **consolas de videojuegos**, televisores inteligentes y otros diseñados principalmente para el entretenimiento y las comunicaciones.

Figura 1. Las tablet PCs comenzaron a formar parte de la tecnología cotidiana. El famoso iPad de Apple es un ejemplo.

En los últimos años se ha comenzado a detectar un **patrón de adicción** relacionado con el uso de las **tecnologías** de la información, que pueden sufrir con mayor probabilidad los menores que los adultos, por su **exposición natural** a ellas. Por tal motivo, es fundamental la **detección temprana** de los **síntomas** que puedan indicar el inicio de una adicción.

CONEXIONES WI-FI PÚBLICAS

Al conectarnos a Internet desde una red de acceso público, como una cafetería o bar, estamos aumentando la probabilidad de que un usuario malintencionado acceda a nuestro equipo, además de que nuestros datos podrían ser leídos por el proveedor de ese servicio. Por lo tanto, debemos evitar utilizar, por ejemplo, homebanking y otros servicios que utilizan información sensible desde este tipo de conexiones.

Entre otras cosas, es importante notar si el **aumento** en el uso de estas tecnologías **interfiere** de manera grave en la **cotidianidad**, haciendo que el menor pierda el interés por otras actividades, evite las **tareas escolares** y actitudes similares. Esto suele traer aparejados **conflictos** con los padres.

Una conducta típica que podría ser indicio de problemas de adicción es la necesidad de **aumentar la duración**, la **frecuencia** o ambas de uso de alguna tecnología, ya sea el teléfono móvil, la consola de juegos, la red Facebook, etcétera. Esto tiene una explicación fisiológica, ya que a medida que el cerebro se acostumbra a lo que lo excita con una determinada **intensidad**, va requiriendo **estímulos** cada vez más fuertes para experimentar la misma **sensación de placer**, por lo que busca aumentar las acciones que la promueven.



Figura 2. Para los niños, la familia es la referencia de la autoestima y la confianza, y fuente de ellas.

CUIDAR LAS CONTRASEÑAS

Las contraseñas (**passwords**) son la primera línea de defensa contra cualquier tipo de ataque a nuestras cuentas, por lo que es importante mantenerlas seguras y lograr que sean diferentes para cada uno de los sistemas importantes que usamos. Además, se recomienda cambiarlas con frecuencia y no anotarlas en ningún lado que pueda ser accedido de manera fácil por otras personas.

También puede ocurrir que el menor **pierda el control** de la actividad, necesitando llevarla a cabo solo por la búsqueda de **alivio** del malestar que le produce el hecho de no hacerlo. Esto está relacionado con el llamado **síndrome de abstinencia**. Además, es posible que, de la misma manera que con otras adicciones, el problema sea **negado** y **ocultado** por el niño, a pesar de las evidencias notables que no pueden ser cubiertas con **mentiras**. Por lo general, el proceso es tan **gradual** que es **difícil detectar** cuándo se está frente al comienzo de un verdadero inconveniente, lo que nos lleva a tener que observar con detenimiento los **indicios** para poder detectarlos lo más pronto posible.

No todos están **expuestos** a la misma probabilidad de desarrollar algún tipo de adicción a las nuevas tecnologías, ya que esto depende en mayor o menor medida de algunos aspectos que podemos agrupar en tres: los **personales**, dado que algunos individuos tienen más tendencia en sí o son naturalmente más vulnerables; los **familiares**, donde se refleja la socialización primaria; y los **sociales**, en el sentido de la influencia que los mensajes exteriores influyen sobre la persona. Podemos decir que estos funcionan como **factores de riesgo** frente a la mencionada probabilidad.



Figura 3. Los riesgos sociales pueden apuntalarse mediante algunos factores de protección, como la autoestima.

Como contrapeso de los factores de riesgo aparecen los **factores de protección**, que son aquellos elementos que contribuyen a la prevención de los problemas relacionados con las nuevas tecnologías.

Entre estos están algunas capacidades personales como la **asertividad**, las **habilidades sociales** y la **autoestima**. Algunas de las habilidades sociales básicas son: saber disculparse; saber emitir opiniones; comenzar, sostener y finalizar una conversación; aceptar críticas; expresar gusto y disgusto; realizar y aceptar cumplidos y saber pedir y cumplir pedidos.

El protagonismo de la PC

La computadora se ha transformado, con el tiempo, en un dispositivo de gran importancia en el hogar, tanto que muchas familias cuentan con **más de una**. En cuanto a su uso, siempre deben tenerse en cuenta los aspectos relacionados con la **seguridad** y la **privacidad**, ya que, en gran medida, la gente desconoce los detalles del funcionamiento interno de los dispositivos electrónicos y del software, lo que aumenta muchas veces el riesgo de ser engañados o ser víctimas de algún **ciberdelincuente** o **usuario malintencionado**.

> SIEMPRE DEBEMOS MANTENER LAS APLICACIONES Y EL SISTEMA OPERATIVO ACTUALIZADOS

Respecto a la seguridad de la PC, siempre debemos mantener las **aplicaciones y el sistema operativo actualizados**. En general, el software da aviso cuando hay actualizaciones nuevas disponibles, y **no debemos ignorar estos mensajes**. Por el contrario, es conveniente acceder lo más pronto posible a la descarga que nos ofrece. Mantener el software desactualizado puede ser una **ventana de acceso** a nuestros datos.

NICKNAMES

Se llama **nickname** (seudónimo o sobrenombre) al nombre con el que se conoce a una persona en Internet, que, por lo general, difiere de su nombre real. En un principio, se utilizaba para identificarse resguardando la identidad, aunque hoy en día también es común que sean equivalentes. Algunas personas han conservado sus nicknames al punto de ser reconocidos en el mundo físico por el mismo sobrenombre.

En cuanto a las **laptops** y **netbooks**, se aplican las mismas medidas de protección que con las computadoras de escritorio, solo que debería tenerse **más cuidado** con la infección de códigos maliciosos, ya que, al estar **transportándolas** y **conectándolas** en distintas **redes inalámbricas**, la probabilidad de tener problemas aumenta mucho. Además, a diferencia que con la PC de escritorio, un tema que debemos tener en cuenta es la **seguridad física** del dispositivo, ya que dada su movilidad, una computadora portátil es **susceptible de ser robada**.



Figura 4. Los **cables de seguridad** para laptops evitan que sean sustraídas cuando se los sujeta a un punto fijo o difícil de mover.

Si bien no hay contramedidas para esto, más que la precaución es importante que estos equipos cuenten con una **clave de encendido** (llamada **password de BIOS**) previa al inicio del sistema, lo cual no



HISTORIALES DE MENSAJES

Una forma de resguardar la privacidad en los equipos es no permitir que los programas de mensajería instantánea almacenen los historiales de las conversaciones que tenemos con nuestros contactos. La desventaja que tiene esto es que no podremos acceder a esos mensajes en caso de quererlo, cosa que a veces es útil para recordar alguna conversación. Esto forma parte de la paradoja de **seguridad versus privacidad**.

evita que sea encendido pero retrasa las medidas de un delincuente para acceder a la información que contiene. También es conveniente que el sistema operativo tenga una **clave de acceso**, aunque solo exista un único usuario, para dificultar aún más la tarea de un potencial delincuente. Por supuesto que existen medidas más complejas para tomar, pero estas **primeras barreras** de protección son sin dudas las más importantes. Incluso, existen algunas herramientas de software que permiten identificar y **rastrear equipos** cuando estos se conectan a Internet o realizar algún tipo de **bloqueo o eliminación** de información de manera **remota** cuando se la reporta como robada. Todo esto puede ser instalado y configurado por un **técnico especializado**.

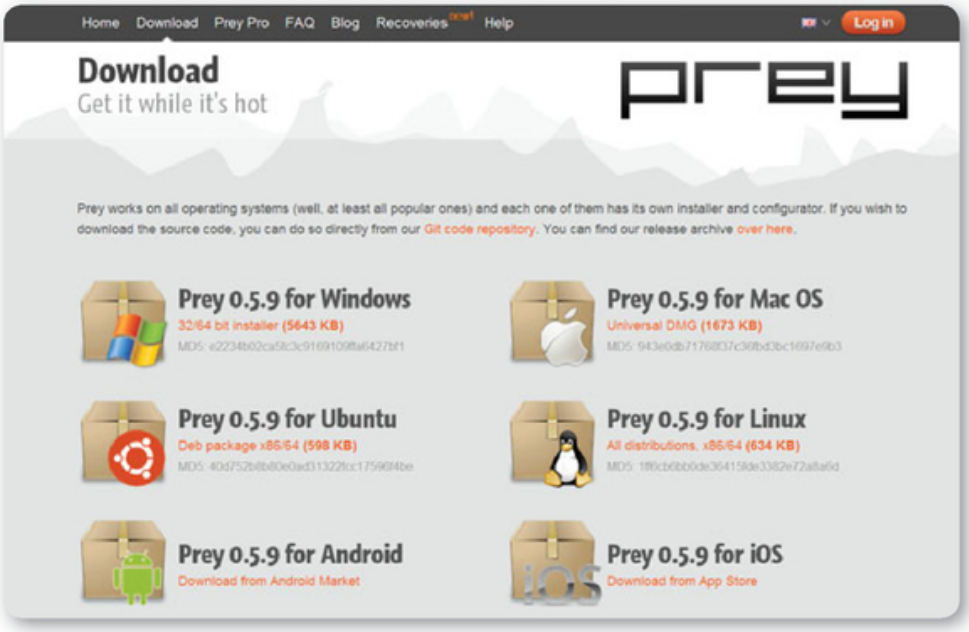


Figura 5. **Prey** es un software gratuito que permite descubrir la ubicación estimada de un equipo robado o perdido.

ACTUALIZAR EL NAVEGADOR

El navegador es nuestra ventana con el mundo virtual, por lo tanto es fundamental mantenerlo actualizado. Al utilizar la versión más reciente estaremos mejor protegidos. Si bien el proceso es distinto en cada navegador, como **Google Chrome**, **Mozilla Firefox**, **Internet Explorer** o **Apple Safari**, todos suelen actualizarse de manera automática al detectar una nueva versión disponible.

Celulares y smartphones

Dado el rol que cumplen los teléfonos móviles en nuestra vida cotidiana, es de vital importancia **mantenerlos limpios** de cualquier clase de infecciones de virus y códigos maliciosos. Si en algún momento detectamos que el dispositivo está funcionando **más lento** de lo normal, que aparecen **pantallas aleatorias** mientras navegamos o lo utilizamos, o recibimos **mensajes extraños**, pueden ser indicios de que estamos siendo afectados por algún tipo de **software malicioso**.



Figura 6. Así como existen los antivirus para PC, también hay versiones para celulares. Un ejemplo de esto es ESET Mobile Security.

Pese a haber sido concebido como un **dispositivo para hablar**, los menores tienen una gran tendencia a utilizar los celulares para enviar **SMS**.

CONTRASEÑAS ESPECÍFICAS DE APLICACIÓN

Google incorpora la posibilidad de generar contraseñas especiales de un solo uso para que sean ingresadas en aplicaciones específicas y así validar nuestra identidad frente a un servicio o aplicación determinada. Una vez ingresada, la contraseña ya no sirve y debe generarse de nuevo si se desea acceder. Esto aumenta de modo sustancial el nivel de seguridad de nuestra cuenta.

En el caso de contar con teléfonos más avanzados (**smartphones**), la tendencia crece hacia el **chat** mediante programas específicos, como **WhatsApp** y **BlackBerry Messenger**; el uso de las redes sociales, Internet y los juegos, tanto **online** como **locales**. También puede que se acceda a lo mismo mediante el uso de una conexión **Wi-Fi** en lugar de una red común con tecnología **3G** o **EDGE**, que son las que se suelen utilizar en telefonía móvil para prestar servicios de **Internet y datos**.



Figura 7. El uso de los celulares debe explicarse con claridad a los menores para que lo utilicen de manera prudente.

La edad a la que los menores comienzan a utilizar su **propio móvil** es cada vez **más temprana**, ya que muchos padres prefieren contar con la posibilidad de **ubicarlos** o **saber de ellos** en cualquier momento, o que los niños puedan llamar si es necesario o están en problemas. Si bien hoy en día casi todo adolescente cuenta con un dispositivo propio, en el caso de los más chicos aún se discute la **edad ideal** de comienzo de uso.

Es importante recordarles a los menores que deben **minimizar** el uso del celular mientras **caminan por la calle**, tanto por la posibilidad de que les sea **arrebatado** de las manos como por el hecho de que los mantiene **distraídos** y pueden sufrir algún **accidente**.

Al irse a **dormir**, se recomienda que el móvil se **apague** para evitar llamadas, alertas y mensajes que puedan interrumpir el sueño. Si es necesario configurar una **alarma**, estas suelen funcionar incluso con el **teléfono apagado**, así que no es motivo para dejarlos encendidos.



Figura 8. Si utilizamos servicios de Google, es importante configurar las contraseñas de aplicación, muy comunes en aplicaciones de celulares.

En muchos colegios contemplan la **prohibición** de utilizar el teléfono celular en el **aula**, por lo que es importante conocer cuál es la política de la escuela a la que acuden nuestros hijos.



Figura 9. En las aulas suele prohibirse el uso de los celulares para que los alumnos se mantengan concentrados en la clase.

En caso de robo, hurto o extravío del dispositivo, debemos considerar que más allá del evidente **costo monetario** del aparato, lo más importante es la **información** que contiene, ya que pueden encontrarse **agendas personales**, **datos privados**, casillas de e-mail, acceso a redes sociales y servicios, archivos y documentos, etcétera. Es por ello que se debe utilizar siempre el **bloqueo del teléfono**, en lo posible habilitado de manera **automática** cuando no se lo esté utilizando.

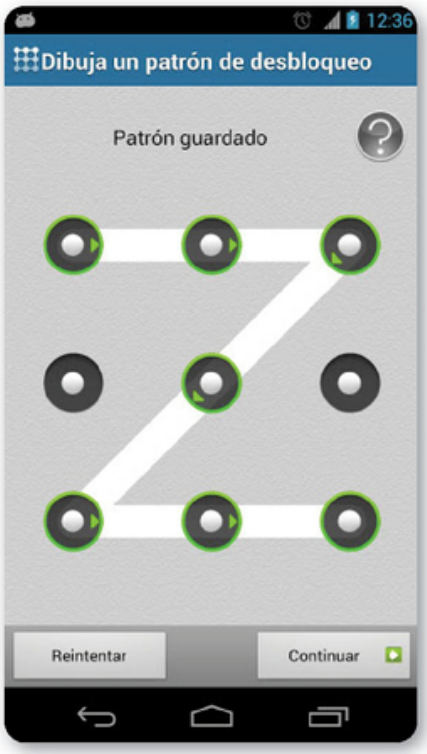


Figura 10. El patrón de desbloqueo visual es un recurso muy útil para prevenir el acceso de desconocidos a nuestro aparato.

Además, siempre se debe tomar como medida preventiva la realización de **copias de seguridad** de la información para evitar perderla (pueden utilizarse los sistemas de sincronización del propio software del teléfono móvil).

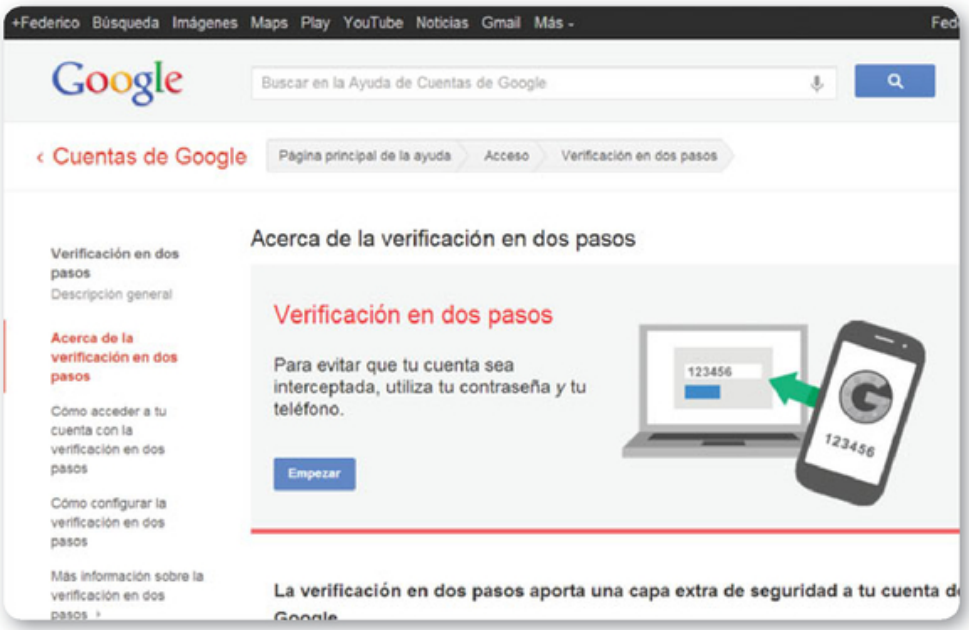


Figura 11. La verificación en dos pasos es un recurso para garantizar que solo nosotros accedemos a nuestra cuenta y requiere un teléfono celular.

Los límites posibles

Establecer **límites y normas** es común en lo que a educación se refiere, ya que los niños necesitan ser **guiados**. Por eso, es de vital importancia tener en claro algunos aspectos de estos límites para que puedan ser **realistas y adaptables**, y que no sea necesario cambiarlos según la circunstancia. De hecho, siempre es conveniente **ser firmes** en las normas, ya que es natural que los niños quieran evadirlas. Sin embargo, sabemos que **no se puede limitar absolutamente todo**, por lo que debe seleccionarse bien aquello que se limitará.

> LOS LÍMITES DEBEN SER ADAPTABLES PARA QUE NO SEA NECESARIO CAMBIARLOS

Según se ha podido determinar a lo largo de los años, cuando los niños **no reciben límites claros** y concisos suelen devenir en **jóvenes inconformistas** e intolerantes de las negativas y circunstancias adversas. Por el contrario, a quienes se les **exige demasiado** y obedecen por **miedo** a ser **castigados**, suelen devenir en **rebeldes** y **transgresores**.

Los límites deben ser conocidos **con antelación** en lugar de esperar que se los transgreda para condenar la conducta. Es conveniente plantear las reglas **en positivo**, evitando empezar por **no** las frases que las representan, además de **recordárselas a los niños con frecuencia** para que las tengan presentes. En muchos casos, se elige **premiar su cumplimiento** mediante el **reconocimiento verbal**.

Es posible que por alguna razón los padres decidan **limitar en exceso** el uso de algunas tecnologías a sus hijos, considerando incluso que eso implicará una gran **diferencia** con sus compañeros y amigos, ya

¿CASTIGOS O NO?

Si bien el castigo no es un método recomendable de enseñanza, a veces es necesario que el menor sepa que puede ser castigado. Por eso, es importante que los niños siempren conozcan las condiciones de antemano, que las medidas que se tomen se apliquen lo más inmediatamente posible, que sean acordes con cada edad y que sea posible cumplirlas.

que tal vez la mayoría esté utilizándola. En estos casos, es recomendable **compensar** esta diferencia con la realización de alguna actividad específica con ellos para que sientan que, aunque se les está **quitando** por un lado, se les está dando **algo muy especial** por otro, algo a lo que quizás sus compañeros no tengan acceso fácilmente. Esto puede ser, por ejemplo, permitirles realizar alguna tarea particular **de adultos** con absoluta supervisión de un mayor, para que comprendan que el objetivo no es castigarlos ni hacerlos sentir menos que el resto, sino que es una **decisión importante** en favor de su bienestar, en base a alguna clase de convicción de la que sus mayores se hacen responsables.



Figura 12. Es bueno escuchar siempre el punto de vista del menor para poder aprender cómo construye su perspectiva.

En cuanto a la **buena comunicación** con ellos, la propia experiencia como padres es una gran herramienta, pero es bueno recordar algunos puntos. Un ejemplo es el caso de las **críticas** que se les hace, que deben centrarse en el **comportamiento** y **no en la persona**. Los temas deben hablarse de a **uno por vez** para asegurarnos de que cada uno haya sido comprendido sin perderse en distintos hilos de conversación. Siempre se debe intentar **ser breve**, **específico** y **concreto**, evitar generalizaciones y cuidar la **comunicación no verbal**. Por otro lado, elegir el **momento adecuado** para un regaño o una conversación puede ser la diferencia entre el éxito y el fracaso.

Es importante aclarar que según algunos estudios, los niños en muchas ocasiones **no hablan** sobre sus actividades en Internet por **miedo** a ser **sancionados**, **culpados** o que se los **castigue** impidiéndoles el uso de la computadora. Por lo tanto, **no puede confiarse** en que ellos iniciarán el diálogo sino que son los adultos los que deben preocuparse por hacerlo.

Consejos para padres

Aunque pueda parecer repetitivo, es fundamental tener en cuenta una serie de recomendaciones que mejorará mucho la experiencia de los menores en Internet y aumentará la tranquilidad de los padres.

Ante todo, es muy importante **hablar abiertamente** de los riesgos con los niños para que poco a poco los puedan ir reconociendo por sí mismos y acepten las medidas que los adultos tomen con el fin de **protegerlos**. En algunos casos es bueno que los consejos también les lleguen por medio de otra persona que no sean los padres, ya que la **mezcla de roles** de autoridad podría derivar en que algo sea incumplido solo porque proviene de los padres.



Figura 13. Algunos servicios como Gmail nos brindan un reporte de la última actividad de la cuenta.

Como ya vimos, establecer **reglas y límites** (consensuados con ellos) para el uso de Internet y los servicios online evita en muchos casos que se transgredan. Es importante contar con **software de protección** de distinto tipo, en especial un **antivirus** y uno de **control parental**, aunque un **firewall personal** suele ser un buen complemento.

> EL ANTIVIRUS Y EL SOFTWARE DE CONTROL PARENTAL SON INDISPENSABLES

Por distintas causas, no es para nada recomendable **prohibir** el uso de las tecnologías a los menores. La primera es que no se los puede controlar todo el tiempo, y ya sea en la escuela, en un cibercafé o en la casa de un amigo podrán **acceder** a las redes sociales, crearse perfiles virtuales y **utilizar** aquello que en su hogar les prohíben. Por otra parte, no es conveniente que se los obligue a estar **marginados de su entorno**, ya que si sus compañeros y amigos frecuentan el uso de distintos sitios y tecnologías comunes (como las redes sociales o los juegos online) y ellos no, se los estaría aislando del estándar de **su edad**. En el otro extremo, tampoco se recomienda permitirles el **libre uso** de las tecnologías sin ninguna clase de supervisión ni control, ya que ellos, por lo general, desconocen los **riesgos asociados**.

Algunas familias realizan una curiosa práctica que es redactar y firmar una especie de **contrato familiar** en el que se **comprometen** por escrito a cumplir con lo que se ha dispuesto para cada una de las partes. Esto es un buen método didáctico para que los menores asuman **mayor responsabilidad** en el uso de las tecnologías y el comportamiento con los demás, apelando a una práctica propia de adultos que probablemente repetirán el resto de sus vidas, como es la firma de un contrato.



FIREWALL, EL FILTRADOR POR EXCELENCIA

Existe en informática un componente conocido como **firewall** (o **cortafuegos**) que se utiliza, ya sea en modo de hardware (un dispositivo independiente) o de software (un programa especial que se instala en el sistema), para proteger las redes y las computadoras de tráfico que pueda resultar potencialmente dañino. Algunos cuentan con versión gratuita, como el famoso **Zone Alarm** (**www.zonealarm.es**).

Hablar con ellos sobre **sus propios hábitos** y costumbres es una buena idea, y también pedirles que nos expliquen cómo se utilizan los diferentes sistemas que manejan, lo que les da la posibilidad de sentir que los **valoramos** y **respetamos** por aquello que saben. Así, por más que ya tengamos esos conocimientos, podemos interactuar más con ellos y permitirles **que nos convenzan** de sus habilidades para el uso adecuado.

En el caso de los más chicos se recomienda que solo puedan navegar en la casa **cuando haya un adulto** a cargo que pueda supervisarlos. De no ser posible, al menos es importante que luego se compruebe lo que han navegado por medio de algún software especializado o consultando el **historial de navegación**. Para hacerlo en Chrome, Firefox y Explorer, solo hay que presionar la combinación de teclas **CTRL + H**. En el caso particular del historial de búsquedas en Google, debemos iniciar sesión y luego ingresar a **www.google.com/history**, como se muestra en la siguiente figura.



Figura 14. Es muy útil la función del historial de búsqueda de Google para conocer la actividad de los menores.

Es recomendable que la computadora que se utiliza para navegar se encuentre en una **zona de uso común de la casa**, como una sala de estar, de manera que quede visible para los mayores.

Siempre que sea posible, es conveniente **conocer las contraseñas** de los menores, al menos hasta que lleguen a la

adolescencia. Este tema es bastante delicado porque, con el tiempo, ellos comenzarán a considerar su **esfera íntima** y no querrán proveernos la información, así que debemos conocer el punto en el que debemos empezar a **respetar su privacidad**.



Figura 15. La computadora debería estar en un lugar de uso común de la casa para que pueda ser vigilada por un adulto.

También es bueno **chatear con ellos** para conocerlos como usuarios y de manera virtual. Asimismo, es ideal estar entre los contactos de las redes sociales y la mensajería instantánea de los menores, aunque muchos prefieren que no sea así.

En lo posible, se debe intentar que el tiempo en el que permanecen conectados no sea en **horarios nocturnos**, ya que los riesgos de hablar con desconocidos adultos aumentan de manera sustancial.

TIEMPO LIBRE

Es fundamental aprovechar el tiempo libre para estimular a los menores y permitirles conocer nuevas actividades relacionadas con los deportes y la vida al aire libre, teniendo en cuenta sus gustos y preferencias, y tratando siempre de buscar espacios para compartir y conocerlos mejor. El entretenimiento y la diversión pueden funcionar como un buen punto de conexión con los niños.

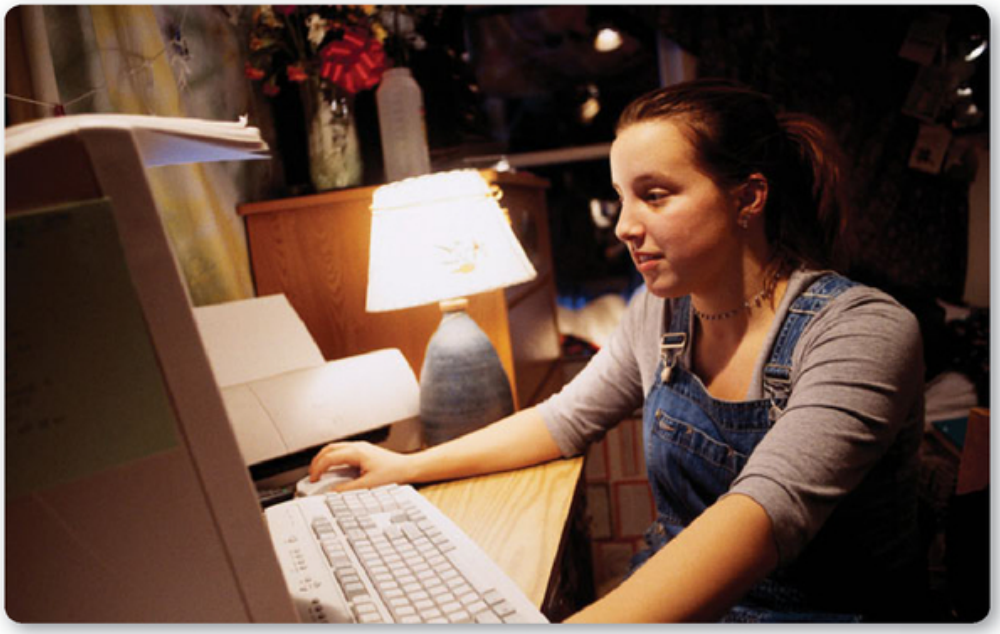


Figura 16. Es importante limitar el uso de Internet en horarios nocturnos, en especial para los más pequeños.

Por sobre todo, debemos intentar **conocer las tecnologías** al mismo nivel o incluso más de lo que las conocen ellos. Esto permite oficiar como **figura de autoridad** en el tema, pero además evita que por alguna configuración o uso avanzado nos dejen sin la posibilidad de **supervisarlos**.



Sobre los menores que suelen utilizar juegos online o de consola, debe tenerse en cuenta que es mejor involucrarse como adulto en la decisión de la **elección de un juego**, sea comprado o descargado, para tener una referencia de la **edad adecuada** que se recomienda, el **tipo de juego**, los términos y las condiciones de uso, y otros detalles que pueden ser de utilidad.

Figura 17. Los juegos de video estimulan algunas capacidades importantes en los niños, pero debe tenerse cuidado de no caer en excesos.

Consejos para menores

Más allá de los **consejos** que sirvan para ayudar a los adultos a encarar la problemática de la tecnología, también debemos tomar una serie de recaudos que incluirán el **diálogo con los menores**, donde los aconsejaremos sobre temas como:

- Que **no crean en todo** lo que ven en Internet, ya que hay mucha información falsa. Pueden buscarse ejemplos puntuales para ilustrar esto. Es bueno además que aprendan a **enfocarse en lo que están haciendo** y que no se dejen dispersar por otras ventanas y contenidos, al menos en un principio, hasta que sepan organizarse.
- Que utilicen **servicios de e-mail conocidos**, ya que para registrarse requieren proveer pocos datos personales y en general permanecen bien resguardados por el proveedor, como **Hotmail** (ahora Outlook), **Yahoo!** o **Gmail**. Es mejor evitar que el nombre de usuario o el alias contengan información personal directa, como la fecha de nacimiento.
- Que **no respondan e-mails** ni mensajes privados en redes sociales en los que se les pida que hagan algo que **no quieren** o les digan algo que los haga **sentir mal**. También que aprendan el uso de la función de **copia oculta**, para resguardar la privacidad de sus conocidos al responder a muchas personas a la vez.

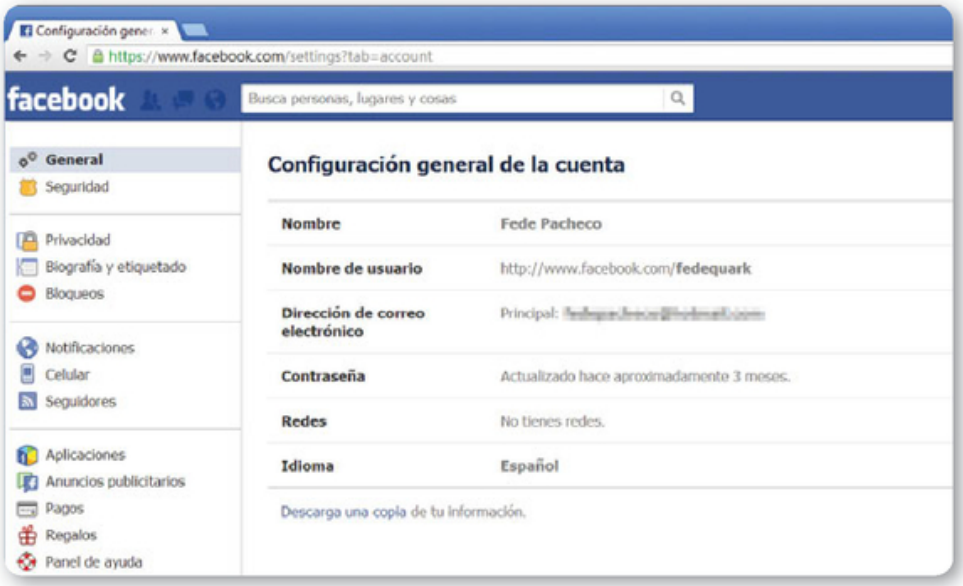


Figura 18. Servicios y redes como Facebook permiten descargar nuestro perfil completo con todo el historial de actividades.

- Que **piensen bien** lo que publican en las redes sociales y los mensajes que envían, ya que estos pueden permanecer en Internet **por más que sean eliminados**, y eso podría causarles inconvenientes personales en el futuro.
- Que **no brinden información personal** a gente que no conozcan **ni hablen con desconocidos** en salas de chat públicas. Que no acepten archivos ni ningún tipo de obsequio virtual.
- Que no fomenten ni adhieran a la práctica llamada **sexting**, que implica el **envío de imágenes** con contenido sexual a través del teléfono celular. Esto es cada vez más común entre adolescentes.
- Que no depositen total confianza en los **videochats** por **webcam**, ya que existen programas especiales que simulan la presencia de un usuario real mediante **videos pregrabados**.



Figura 19. Nadie debería comportarse en Internet de una forma que no lo haría fuera del ámbito virtual.

- Que aprendan a elegir **contraseñas seguras**, evitando datos personales directos, utilizando **mayúsculas** y **minúsculas**, combinándolas con **números**, **reemplazando** números por caracteres y, por supuesto, que no las compartan con nadie. Esto último no es un detalle menor, ya que los niños no conocen los límites de la confianza. Además, es común que a modo de juego los chicos se roben las contraseñas entre ellos, aunque a veces lo hacen de manera maliciosa o para **demostrar superioridad** en el uso de las computadoras.

Sobre el acoso online

Para manejar la **intimidación** y el **acoso online**, tenemos que ser claros con las recomendaciones para que los menores sepan cómo actuar al respecto. En primer lugar, deben **saber decir que no** y pedirle a la persona que les **deje de hablar** y no vuelva a contactarlos. Si aun así continúa, deben saber que tienen que **avisarle a un mayor**.

También tienen que aprender a **no responderle** más en ningún contexto, ni los chats ni los e-mails, sin importar lo que diga y, si es posible, que **bloqueen** o **eliminen** el contacto correspondiente. Al ver un comportamiento adecuado del niño, un acosador suele entender que el menor está informado sobre cómo actuar y deja de acosar por su propia protección. En caso de que un menor nos avise de esto, debemos **consultar los chats** y de ser posible **imprimir una copia** como evidencia. Si se tienen mensajes en el **buzón de voz**, es mejor mantenerlos guardados hasta que se resuelva el tema y si fuera posible, realizar una **grabación** del audio en algún medio.

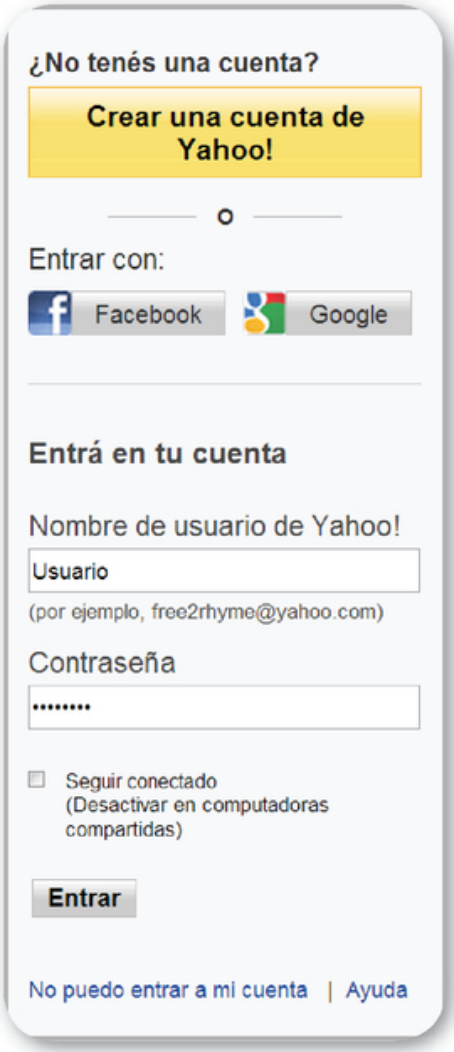


Figura 20. Debemos enseñarles a los menores a utilizar contraseñas seguras.

Algunas **señales del comportamiento** de los menores deben ser especialmente tenidas en cuenta para detectar posibles problemas de **acoso virtual** (**grooming**). Por ejemplo, es común que el menor en el fondo sepa que **no debería** estar hablando con una persona mayor (si es que ya está en esa fase del relacionamiento) y quiera **ocultarlo** a sus padres. Entonces, por ejemplo, **cambiará repentinamente de pantalla** ante la llegada de un adulto para que este no vea qué hace.

También debemos estar atentos a las **llamadas sospechosas**. Si bien el **identificador de llamadas** ayuda mucho en este sentido, el acosador por lo general sabe de esto y busca la manera de ocultar la

procedencia de su llamada utilizando un teléfono público. A veces, el menor permanece **conectado hasta altas horas** de la noche y escribe más de lo que navega, algo común en el chat con acosadores. Por ese motivo, lo mejor es definir un **horario límite** para el uso de Internet y la computadora. Se debe también prestar atención a cualquier clase de **regalo** (tecnología, ropa o lo que fuere) que el niño reciba, ya que podría haber allí un vínculo con un mayor.



Figura 21. Es importante explicarles a los niños cómo reaccionar ante el acoso online.

Además, es normal notar que ante casos de **grooming** los niños estén **inusualmente molestos** por alguna eventual **interrupción del servicio** del proveedor de Internet. Finalmente, algo tal vez menos evidente y más progresivo es que se produzca un **distanciamiento de su entorno** cercano de amigos y familiares.



PREDICAR CON EL EJEMPLO

Cuando los niños ven que sus padres utilizan constantemente el teléfono móvil o que tienen comportamientos cotidianos nocivos relacionados con el uso de la tecnología (y también sin ella), tienden a tomar como modelo tales conductas y pensar que eso es lo correcto, ya que aún no tienen sus propios criterios formados.

Ante cualquier duda, por supuesto, lo ideal es que siempre **consulten con un adulto** aunque deban esperar un tiempo hasta que llegue o que simplemente tarde en responder debido a sus ocupaciones. Es bueno que los niños aprendan a regular desde el comienzo la **ansiedad** por las respuestas, dado que **Internet y la tecnología promueven la inmediatez**, por lo general, bastante irreal y exigente para las personas.



Figura 22. Los menores deben saber que cuentan incondicionalmente con los adultos ante cualquier duda que tengan.

RESUMEN

En este capítulo analizamos la perspectiva específica de los padres de familia en cuanto al uso de las tecnologías de la información por los menores. Así, abordamos el tema del hogar moderno con sus características singulares respecto a épocas anteriores y estudiamos algunas de las tecnologías presentes en casi todo entorno familiar. Analizamos algunas situaciones particulares en las que es necesario definir límites y describimos cómo mejorar el acercamiento a los menores mediante la comunicación efectiva y asertiva. Por último, vimos una lista de recomendaciones puntuales para padres que pueden ayudar con algunas decisiones cotidianas.

Actividades

TEST DE AUTOEVALUACIÓN

1. Identifique qué tecnologías se utilizan en su propio hogar y determine la que considere más riesgosa en cuanto al uso por parte de los menores.
2. Pida a su hijo, sobrino o cualquier menor de su familia o de una familia cercana de confianza (con autorización de sus padres) que le expliquen alguna funcionalidad de Facebook, Twitter o algún juego online que utilicen normalmente.
3. Utilice alguna de las redes sociales más populares (Facebook, Twitter, etcétera) para conectarse con grupos de padres que traten sobre los riesgos en el uso de las tecnologías entre los menores.
4. Organice una conversación familiar para hablar del tema del uso de las redes sociales y comunique a los menores algunos de los consejos que le hayan resultado importantes, previo consenso entre adultos.
5. Comparta los consejos y recomendaciones que le resulten más útiles con otros padres de familia que puedan estar preocupados por la misma problemática.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

*06

Desafíos del educador

En este capítulo plantearemos algunas de las principales problemáticas asociadas a la tecnología desde el punto de vista del educador para distinguirlas de los temas que están más propiamente relacionados con el entorno hogareño. Analizaremos también las tecnologías como parte activa del proceso educativo.

- Evolución y panorama de la educación 126
- Tecnologías educativas 132
- El nuevo rol del docente 135
- Internet y tecnología en la escuela 139
- Consejos para docentes 144
- Resumen 147
- Actividades 148

Evolución y panorama de la educación

Está claro que para enfrentar y **resolver los problemas** relacionados con la educación, es necesario que ciertas deficiencias del tipo social estén, cuanto menos, en vías de ser solucionadas. Es por esto que cualquier **política educativa** que se precie de tal y tenga como objetivo real un **cambio sostenible** de largo plazo debe estar alineada con una **política social** que garantice, en primera instancia, el acceso al alimento y al agua potable, algo que muchos de los sectores menos beneficiados ni siquiera poseen. Recién cuando se haya asegurado el acceso a los **elementos básicos** para que una sociedad sobreviva, los gobiernos deberán proveer un **sistema de salud efectivo** que permita a las personas evitar el sufrimiento por las enfermedades que pueden ser prevenidas, tratadas y curadas. Es entonces cuando un **sólido sistema educativo** puede tener lugar, cuando los niños no deban ir a la escuela por un plato de comida, para que sus padres reciban el dinero de un **plan social**, para que estén **ocupados** una parte del día mientras sus padres trabajan o para recibir los **valores fundamentales** que deben ser provistos en el seno de la familia.



Figura 1. Un sólido sistema educativo debe estar sustentado sobre la base de un eficiente sistema de salud y alimentación.

Un sistema educativo integral deberá **atender las necesidades del niño**, prepararlo sanamente para el tránsito por la adolescencia, brindarle las herramientas para su desarrollo en la juventud y servir de guía en el camino hacia su madurez adulta. Además, en el futuro aparecerán, como en cada época, problemas **propios de los tiempos** que corran, por lo que todos los anteriores inconvenientes deberían estar **resueltos** o al menos en camino de ser solucionados.

Desde antes de la modernidad se marcó una gran diferencia entre **personas educadas** y personas que no lo eran. Conforme avanzamos, nos estamos moviendo hacia un lugar en donde cada uno será muy diferente, porque **habrá tomado caminos distintos** para llegar a donde está y no será comparado de manera directa con sus pares, sino a través de su **capacidad de llevar a la acción** aquello que tiene el potencial de realizar. Esto marcará la diferencia más que nunca, y tal capacidad de actuar y obtener resultados será sin lugar a dudas **el don más preciado**.



Figura 2. Por décadas se ha fomentado la competitividad en los niños, lo que se tradujo en grandes frustraciones durante la edad adulta.

EL ERROR DE LA FRAGMENTACIÓN

Uno de los problemas que más ha minado la educación es el del conocimiento fragmentado, es decir, la separación estanca entre las disciplinas que impide vincular las partes y las totalidades. Así, el futuro deberá incluir un aprendizaje capaz de transmitir conocimientos en contexto y enseñar métodos que permitan comprender las relaciones recíprocas entre las partes y el todo.

Información y contenidos

La **era de la información** ha llegado con algunos cambios que son todavía difíciles de tratar. Pongamos por caso el hecho de realizar un trabajo de investigación o una tarea que incluya la búsqueda de información. Hasta fines de los años 90, el hecho de **buscar en Internet** todavía era una rareza, y se consultaba principalmente en enciclopedias, libros especializados y miles de volúmenes de texto escrito contenido en **bibliotecas**. En menor medida, con el tiempo, comenzaron a consultarse las **enciclopedias digitales**, como la famosa **Microsoft Encarta**. Ya en esa década, la introducción de los soportes digitales para el acceso a la información había sido un gran cambio y, desde el punto de vista de un docente, la perspectiva también se transformaba, ya que se creaba el nuevo flagelo del maestro: **copiar y pegar** (*copy and paste*). Antes de esta práctica, la transcripción de textos obligaba al menos a **procesar la información** y la gravedad era menor. La comodidad introducida por las computadoras en el acceso a los textos digitales dio comienzo a una era en la que saber **de dónde** se obtiene la información deja de ser el problema para convertirse en otro: todos los **resultados** serán **muy similares** entre sí. Esto también derivó en trabajos prácticos y deberes escolares en los que se **redujo el esfuerzo** de la investigación y la lectura para pasar a **confiarse** en las enciclopedias digitales.



Figura 3. El uso de la tecnología ejerce una gran atracción en la atención de los menores.

Pero esto no finalizó allí, ya que la masividad de Internet y de lo gratuito hizo que esas enciclopedias digitales dejaran de ser tan importantes y se pasara a un **modelo de información más viva y en línea**. Esto derivó en la existencia de fuentes online, algunas oficiales de empresas e instituciones y otras en modo de sitios personales y blogs. El caso de **Wikipedia** (**www.wikipedia.org**) es el más conocido, ya que hoy en día cuenta con más de **20 millones de artículos en 282 idiomas y dialectos** redactados por voluntarios de muchos países. Wikipedia nació en el año 2001 y, en la actualidad, es la mayor y más masiva obra consultada en Internet, se encuentra entre los diez sitios más visitados del mundo. Tal explosión no tardó en echar por tierra a las enciclopedias digitales, que fueron desapareciendo poco a poco, como sucedió con Microsoft Encarta, que funcionó entre los años 1993 y 2009.



Figura 4. Inspirado por las ideas de Ayn Rand y su filosofía objetivista, Jimmy Wales creó Wikipedia, la enciclopedia libre más grande del mundo.

El impacto de las tecnologías en la industria de los textos se ve reflejado en un caso emblemático, el de la **Enciclopedia Británica**, la más antigua en idioma inglés. Tras **242 años de existencia en papel** decidió dejar de imprimirse, y su última edición física fue la de 2010 (en 32 volúmenes). A partir de ahora, la Enciclopedia Británica, que fue **la primera en llegar a Internet**, permitirá el **acceso pago** a su versión digital online, actualizada a diario.

EL PROYECTO SEGU-KIDS

Un completo recurso de referencia en español sumamente recomendable es **Segu-Kids** (**www.segu-kids.org**), un proyecto orientado a la seguridad de menores en Internet que está vinculado a la mayor comunidad de seguridad informática de habla hispana: **Segu-Info**. Desde allí, es posible acceder a textos, descargas y recomendaciones sobre el tema específico de menores en Internet.



Figura 5. La Enciclopedia Británica dejó de imprimirse en 2010, hoy solo se puede consultar online.

Con este panorama, el educador ya no puede contar con que el **esfuerzo** de sus estudiantes se centre en la **búsqueda de información**, sino que debe migrar a una metodología donde el esfuerzo esté puesto en saber **reconocer la calidad de los contenidos** que se encuentran.

La dificultad de garantizar la calidad fue justamente una de las críticas que se le han hecho a Wikipedia y otras fuentes online, lo que derivó en algunos cambios en la manera de **editar artículos** y otras modificaciones que hacen que cada día se encuentre información **más completa y mejor** en esta gran enciclopedia que se crea de manera colaborativa.

HISTORIALES DE MENSAJES

Entre los 6 y los 12 años, los niños comprenden que sus pensamientos y sentimientos difieren de los de los demás, y se hacen más conscientes de sí mismos. Además de ser la fase de los **por qué**, en esa etapa es cuando adquieren el sentido de su propia eficacia, de pertenencia a sus primeros grupos y de responsabilidad individual. Por estas razones, es fundamental moderar nuestras expectativas sobre ellos para evitarles frustraciones.



Figura 6. Wikipedia representó una verdadera revolución en cuanto a la información enciclopédica en Internet.

A nivel **académico**, uno de los temas candentes en toda conferencia internacional sobre educación es el de la dificultad para **comprobar la copia de textos**, trabajos e investigaciones. Esto responde a una problemática actual que es la gran **cantidad de información** existente, que no puede consultarse si no está indexada.

Además, si la información se encontrara repetida en otro lugar, podría dejar de reconocerse como original entre todas las copias. Por eso, la información encontrada en Internet intensifica el problema de la **comprobación del plagio** y la copia de ideas y textos. Detectar esta práctica es algo complejo y, muchas veces, ni siquiera es posible hacerlo.

> SI LA INFORMACIÓN NO ESTÁ BIEN INDEXADA, NO PUEDE SER ENCONTRADA NI CONSULTADA

Un posible enfoque para dar solución a este grave problema no debería estar basado exclusivamente en las tecnologías y las técnicas de comparación, sino más bien en la correcta **educación de las personas que producen los textos** para que no caigan en la copia como recurso para generar nuevos contenidos. Es importante conocer los derechos de los autores del contenido para poder explicárselos a los alumnos y así eviten robar material.

Tecnologías educativas

En los próximos años, llegarán a su etapa de madurez conceptos como el de **realidad aumentada**, que implica la superposición del mundo real y el digital, pero no con fines comerciales como se usa en la actualidad sino para proporcionar experiencias más completas de aprendizaje. Otra tecnología que llegará a su madurez será la de las **pantallas flexibles** (**OLED**), que permitirán reproducir imágenes sobre un material delgado y flexible, adaptable a las necesidades de los contenidos educativos.



Figura 7. La realidad aumentada permite agregar información virtual a las experiencias del mundo físico.

Los **libros electrónicos** (**e-books**) continuarán su crecimiento, logrando agregar valor a los contenidos escritos por medio de las

DE 12 A 16

Entre los 12 y los 16 años aparece en los niños la necesidad de **autonomía**, la búsqueda de la propia **identidad** y el **egocentrismo**, pero también la fuerte influencia de sus pares y la tendencia a exponerse a riesgos, lo que los transporta a través de la adolescencia hacia la edad adulta. Esta etapa es de suma importancia también en su desarrollo emocional.

tecnologías digitales. Estos podrán funcionar no tanto como un reemplazo sino más bien como una **cómoda** y más **económica alternativa** a los tradicionales libros impresos.

Entre los conceptos más interesantes promovidos por la tecnología de **cloud computing** estará el de los **entornos colaborativos**. Esto significa que profesores de distintas escuelas, en lugares diferentes, podrían coordinar trabajos en conjunto sobre temas que se traten en el aula, lo que además motivará la integración cultural y las experiencias sociales entre los estudiantes.



Figura 8. Kindle, el dispositivo lector de libros electrónicos más famoso, popularizó el concepto de tinta electrónica.

Las **plataformas virtuales** de colaboración **en la nube** serán la clave de este cambio, ya que permitirán y simplificarán el intercambio de ideas, videos, textos e imágenes.

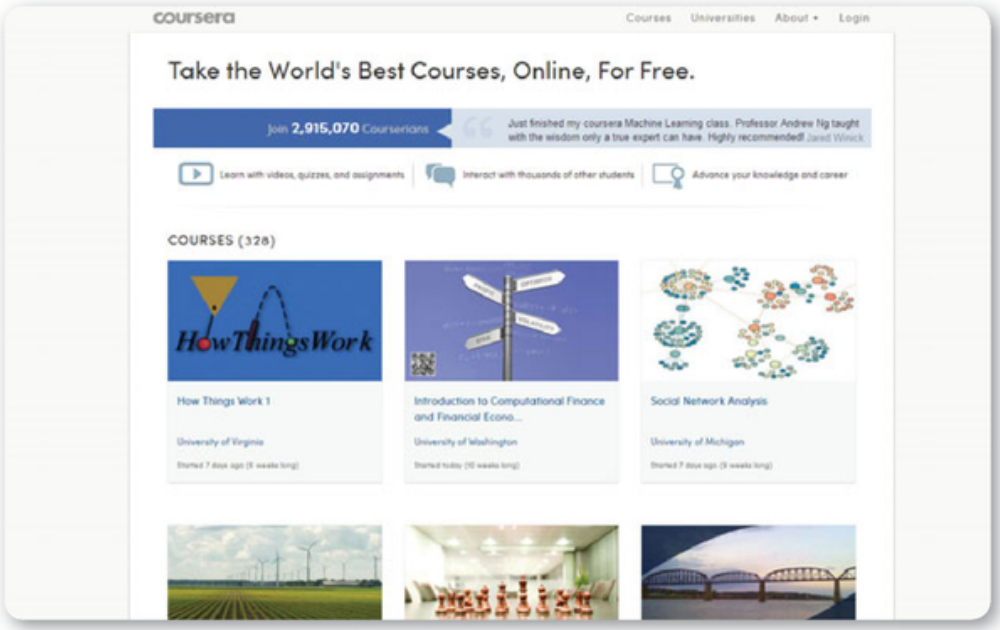


Figura 9. Coursera (**www.coursera.org**) es uno de los proyectos más importantes del mundo en educación online.

El desarrollo de **recursos educativos** accesibles por Internet de manera **abierta y gratuita** (*open content*) permitirá ampliar el alcance de la información hacia todos los niveles de enseñanza y reducirá las brechas entre quienes pueden pagar una educación privada de alto nivel y quienes no. Sin necesidad de mirar tanto hacia adelante, ya en la actualidad podemos encontrar proyectos destinados a la educación global a través de cursos denominados **MOOC** (**Massive Open Online Courses**), que implican una tecnología que permite acceder a videos y clases de cursos específicos de manera abierta, libre y gratuita para obtener información de la mayor calidad, como la de las universidades de **Stanford**, **MIT** (**Massachussets Institute of Technology**), **Harvard** y **Pennsylvania**, entre otras.

LOS CURSOS ONLINE AMPLÍAN EL ALCANCE DE LA INFORMACIÓN HACIA TODOS LOS NIVELES

En los últimos años, se han sumado a esta ola proyectos en español que ofrecen contenidos exclusivamente en habla hispana organizados en universidades de **Iberoamérica**.

La tecnología mencionada es accesible de manera directa por Internet y solo es necesario contar con un **navegador web** y dedicación para tomar los cursos, sin límite de edad ni prerrequisitos. Quizás este sea uno de los primeros intentos reales del ser humano de **socializar** una parte de la educación para que deje de ser **privilegio** de unos pocos.

Si bien estos cursos se orientan más bien al nivel universitario, también hay otros que lo hacen al nivel medio de enseñanza, como el pionero **Khan Academy** (**www.khanacademy.org**) y algunos que le han seguido los pasos, como **Educatina** (**www.educatina.com**) y **Educabilia** (**www.educabilia.com**).

UNIVERSITARIO

Algunos de los proyectos que cumplen con las características de los sistemas MOOC son **Coursera**, **Udacity** y **edX**, que han sido los primeros en apuntar a esta idea ofreciendo contenidos de calidad para tomar libremente por Internet. En habla hispana existen proyectos como **Acámica** y **MiríadaX**, orientados a contenidos de universidades iberoamericanas.

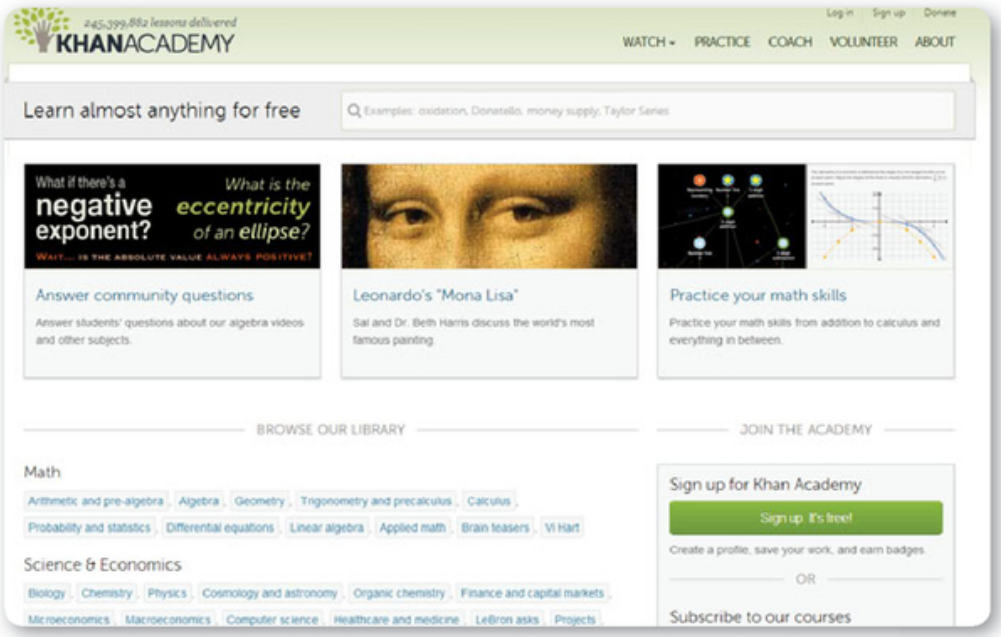


Figura 10. Khan Academy fue el primer proyecto de cursos online especializado en temas escolares para menores.

El nuevo rol del docente

Los grandes **cambios de paradigmas** que se han dado en las últimas décadas en base al desarrollo tecnológico nos presentan una perspectiva de futuro nunca antes vista. Se avecinan tiempos en los que la educación podrá ser más **completa e integral**, y podrá estar tan personalizada como cada individuo requiera para su formación.

En el futuro, los maestros y los profesores pasarán de ser figuras de **autoridad rígida** y absolutista, que imparten una disciplina estricta e inapelable, a formar parte de un **proceso de aprendizaje**

EDUCACIÓN EN EL PASADO

Los siglos anteriores enmarcaron la educación en sistemas estrictos, con regímenes provenientes del ámbito militar, donde se dividía al alumnado por sexo, edad, asignatura, actividad, clase social; y donde el hecho de segregar y dividir constituía en sí mismo la base del sistema. Hoy, pese a los grandes avances, no se ha cambiado demasiado.

conjunto, más lejos de decirle al estudiante qué es lo que debe saber y más cerca de aprender con ellos, aunque se trate de aprendizajes distintos.

El **educador moderno** y de cara al futuro **debe agregar valor** respecto a un libro, a una grabación de audio e incluso a un video de sí mismo explicando los mismos temas. Para que la figura del docente tenga sentido, deberá ser **guía en el proceso de aprendizaje** y no una referencia definitiva ni una figura de autoridad y de conocimiento supremo.



Figura 11. El educador moderno solo será útil si agrega valor en el proceso educativo; ese será su principal desafío.

El educador deberá ayudar a verificar la veracidad de la información encontrada, enseñar a contrastar opiniones, guiar en el proceso de **toma de decisiones** y, en especial, **motivar** en los estudiantes la creación de nuevos contenidos. En un paso posterior, ni siquiera podrá conformarse con ser generador de contenidos, pues lo siguiente será **involucrarse en el diseño** de las plataformas que lo van a distribuir, ya que al fin y al cabo estas son grandes **condicionantes** de los hábitos psicosociales y culturales. El hecho de que el medio y el mensaje estén tan íntimamente relacionados nos lleva hoy más que nunca a validar la más famosa cita de **Marshall McLuhan**: **"El medio es el mensaje"**.

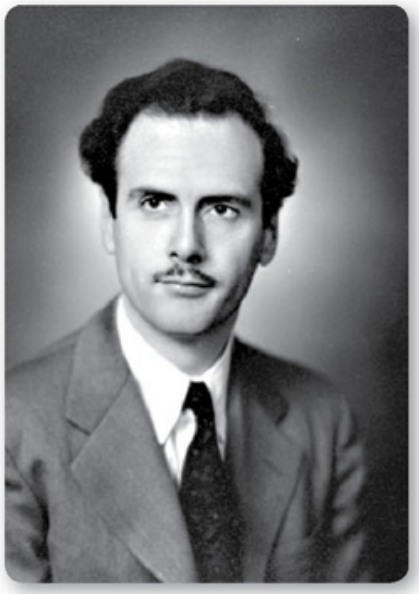


Figura 12. Marshall McLuhan, educador canadiense, creador del concepto de la **aldea global**, inmortalizó la frase: **"El medio es el mensaje"**.

Como educadores, debemos **prepararnos** para estos nuevos escenarios, cual leñador que invierte gran parte de su tiempo **afilando su hacha**, pero no podemos dejar que este pase porque el futuro ya está aquí haciéndose cada día más presente. Debemos **reconocer** que no lo sabemos todo y que Internet será parte de nuestro futuro, por eso, debemos **promover** el uso del **espacio cognitivo** ahorrado por el cerebro al no tener que recordarlo todo para transformarlo en algo más productivo que simplemente almacenar información.



Figura 13. Los sistemas educativos actuales provienen de un modelo militar-industrial y han quedado obsoletos para el futuro.

Los profesores del futuro no podrán contar con su conocimiento estático como **único recurso** ni los estudiantes dependerán de la información en crudo para aprender, por lo que los niños

desarrollarán cada vez **más rápidamente y más pronto** la capacidad de interpretar y aprender por su cuenta. Esta tendencia se reflejará en los **sistemas de autoaprendizaje**, que motivarán en especial a los jóvenes a independizarse de las estructuras tradicionales para su formación profesional. En esos casos, el profesor deberá aprender a **ser un guía** en el **proceso de aprendizaje**, alguien que por conocer el camino que el educando está transitando puede **identificar** el lugar en el que se encuentra, sus posibles **problemas**, **errores**, **trabas** y **preconceptos** débilmente adquiridos o ausentes; no solo ser una fuente de conocimientos.



Figura 14. El docente que todo lo sabe se está convirtiendo en un modelo cada vez más lejano.

Por último, pese a la dificultad que implica **evitar manifestar** y transferir los **problemas personales** de uno mismo a los demás, es fundamental que el educador realice profundos **trabajos internos** para no transladar de ninguna manera sus propias **frustraciones** y **traumas** a los estudiantes. Esto último muchas veces se refleja en el **maltrato a los alumnos** ejercido por los maestros y profesores, que, si bien en otra época pudo ser útil, en estos tiempos en los que el concepto de **autoridad** se reescribe a diario, la **disciplina** debe impartirse por medio de la búsqueda del **respeto**, que solo se logra a través de la **confianza**. Como reza un viejo adagio: **quien es congruente es confiable,**

quien es confiable, es creíble. Esto sin duda es parte del hecho de **reconocer** la verdadera **responsabilidad** que implica continuar siendo docente en los tiempos que están por venir.

Internet y tecnología en la escuela

Los **establecimientos educativos** forman parte activa del entorno cotidiano de los menores, y la **experiencia** que estos tengan en ellos marcará en gran medida la forma en que se comporten fuera. Internet no es ajena a la escuela en tanto que es parte del mundo y se le da un **uso cotidiano**, aunque muchas veces por problemas de **infraestructura** o **recursos** no es posible contar con una conexión en los colegios e instituciones educativas.



Figura 15. El educador debe conocer los riesgos del uso de las tecnologías para poder aconsejar a los estudiantes.

Es importante que los docentes conozcan las **principales tecnologías** con las que interactúan con frecuencia los niños, y las redes sociales son el caso más emblemático. En este contexto, se

está tendiendo hacia una **aceptación** de que estas ya forman parte del entorno y, por consiguiente, comienza a aparecer su uso como **herramienta didáctica**. De esta manera, un colegio podrá tener una **política** de aparición de la institución en las redes sociales, contando con perfiles, páginas y **permiso oficial** para que los profesores puedan utilizarlas en el ámbito del aula. Si la escuela no se adapta a las redes sociales, tarde o temprano, quedará segregada de lo que los niños consideran ya un mundo muy real y siempre presente.

No olvidemos que las redes sociales conforman un punto importante de la **formación de la identidad de los menores**. Su uso incluye sumar amigos, tener contactos y hacer publicaciones en referencia a sus gustos y preferencias, con el objetivo inconsciente de **demostrar valores**, **roles sociales** y **vínculos**. No por casualidad, esto coincide con un contexto histórico de **debilitación** constante de las **instituciones** tradicionales, por lo que los jóvenes tienden a buscar **puntos de referencia** en los ámbitos que se sienten más seguros y familiarizados.



Figura 16. Muchos colegios cuentan con página oficial en Facebook, lo que los acerca más a su propio público.

En los colegios que tengan **informática** o **computación** como materias o utilicen laboratorios de computadoras para ciertas actividades, es fundamental ponerse en contacto con los **profesores** de esas asignaturas o con el **encargado del aula de computadoras**.

Esto puede servir para tomar conocimiento de las tecnologías que se utilizan, la existencia de filtros de contenido y otros controles, y demás temas relacionados con el uso de los equipos. En efecto, cuantos más **espacios de uso de tecnología** en grupos existan, más serán las posibilidades de hablar con los alumnos sobre los temas, debatirlos entre todos, intercambiar opiniones, etcétera.

Más allá de la importancia de **hablar con los menores** sobre la violencia y el trato a través de Internet, de más está decir que la temática debe ser abordada en su **espectro completo**, y no restringido al aspecto informático. Este es un buen **punto de partida** para conocer la manera en que actúan, en general, en sus vidas, sus realidades familiares y otras cosas que surgen de escuchar a un niño.



Figura 17. Proponer actividades que impliquen la búsqueda de contenidos en Internet es positivo si luego se analizan y comparan los resultados.

Puntualmente, para el caso de los **adolescentes**, es tiempo de que comiencen a entender las **obligaciones**, **consecuencias** y **responsabilidades** que pueden devenir del uso de las tecnologías. Por ejemplo, hoy en día se sabe que casi la mitad de las consultoras de **búsqueda de personal** y las áreas de **recursos humanos** de las empresas realizan **consultas en Internet** antes de contratar o entrevistar a los postulantes. Esto excede en algunos casos el uso de las redes especiales de negocios y de búsquedas laborales alcanzando

a otras, como Facebook y Twitter. De esta manera, las empresas podrían comprobar si la persona, pese a lo que diga en su **currículum vítae**, realiza actividades que no son consideradas adecuadas para el comportamiento **dentro de la organización** en cuestión.

En pocas palabras, y expresándolo de otro modo, colocar **fotos** en Facebook donde se ven las borracheras con amigos podría parecer **gracioso** en el momento, pero dentro de algunos años eso mismo podría **dañar una reputación** y definir si alguien es contratado para un determinado puesto de trabajo o no. Como se suele decir: debemos aprender a cuidar el presente porque en el futuro será su pasado.

> SUBIR FOTOS A FACEBOOK PODRÍA DAÑAR UNA REPUTACIÓN SI NO SOMOS CUIDADOSOS

En los tiempos que corren, dada la delgada línea que separa lo **público** de lo **privado** y lo **permitido** de lo **prohibido**, más la **contaminación** existente en el universo virtual, se ha creado una especie de **fantasía exhibicionista** en la que la existencia y el reconocimiento aparecen solo si nos mostramos y aparecemos en Internet. Tal comportamiento habla mucho del sentido en el que estamos evolucionando socialmente y nos deja bastante para pensar en cuanto a la **necesidad de privacidad**.

Algunos temas que los educadores no pueden desconocer respecto al uso de las redes sociales y otros espacios virtuales son, por ejemplo, la necesidad de saber manejar las **configuraciones de privacidad**, el **estilo** y las **buenas prácticas** de uso, los **tips de seguridad** y las **funcionalidades** que pueden aprovecharse en favor de la educación.

En el caso particular de Facebook, dado su enorme impacto en las relaciones y en la forma de comunicarse en el mundo, se cuenta desde

LA FIESTA DE KEVIN

En el año 2007, el joven estadounidense Kevin Colvin pidió unos días en su trabajo para viajar por problemas familiares de fuerza mayor. Tiempo después, la gente de la empresa encontró fotos suyas en Facebook donde se lo veía en una fiesta disfrazado, lo que provocó su despido. Esto complicó su reputación para el resto de su vida, todo por la imprudencia de una simple publicación.

la propia red social con una serie de **directivas** y **recomendaciones** para distintas ocasiones. Con aproximadamente **mil millones de usuarios**, Facebook es sin dudas la red social **más popular** del mundo. No obstante, se calcula que el 10% de los **perfiles** existentes son **falsos**. Esto podría no ser preocupante en principio, pero si tenemos en cuenta que ninguna persona en su sano juicio cometería actos delictivos o abusivos con su **cuenta personal real**, la cifra cobra mayor importancia. Sin embargo, muchos usuarios, ya sea por desconocimiento, inconsciencia, vanidad o simple desinterés, utilizan **su propio perfil** incluso para **actividades non sanctas**.

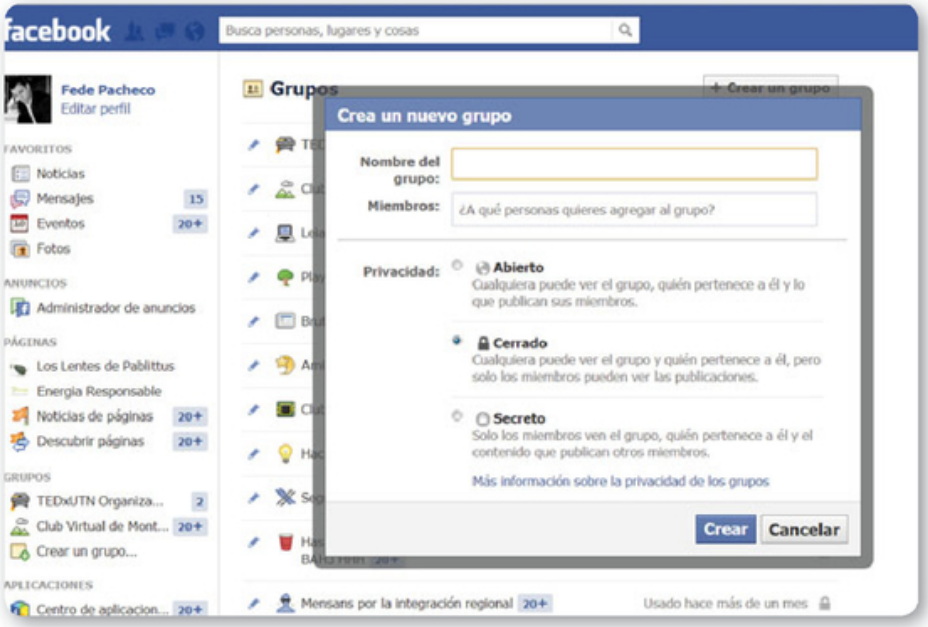


Figura 18. En algunas instituciones se utilizan cada vez más los **Grupos de Facebook** para interconectar a los estudiantes. Es importante controlar su privacidad.

En **Latinoamérica**, la penetración de Facebook supera el 35%, y en algunos países como **Argentina**, **Uruguay** y **Chile** incluso **supera el 50%**. Si bien esta red no permite la creación de perfiles de personas **menores de 13 años**, es imposible controlar la veracidad de la información brindada, por lo que muchos menores de edad ingresan a **edades más tempranas**. Según sus **propias estadísticas**, casi el 10% de los usuarios de la red social son **menores de 17 años**, lo que la establece como la plataforma preferida tanto para jóvenes y adultos como para niños y adolescentes.

Consejos para docentes

Dada la complejidad del abordaje de esta problemática en la actualidad, en muchos casos la manera más efectiva y garantizada (aunque quizás no tan rápida) de conseguir los objetivos es **concientizar a los menores** en lugar de tener que **controlarlos**. De esa manera, en cuanto ellos mismos reconocen el riesgo, ya no es necesario estarles encima con las recomendaciones, que los **adolescentes** toman como algo **fastidioso**. La dificultad es que este método no puede, en general, aplicarse a casos puntuales ni al **corto plazo**, por lo tanto si el problema ya está detectado es mejor **tomar medidas técnicas** y en paralelo concientizar.

En este sentido, en muchos países hay **organizaciones abiertas e independientes** de toda empresa privada que brindan **charlas de concientización gratuitas** para estudiantes de todas las edades, padres y docentes. Una de las más reconocidas internacionalmente es **ISSA** (**Information Systems Security Association**), que tiene representación en muchos países del mundo, incluyendo Argentina, Chile, Brasil, Uruguay y otros de Latinoamérica. Los colegios o docentes que deseen organizar charlas de este tipo solo deben contactarse mediante el formulario online que se encuentra en su sitio web o en el sitio de cada país (**www.issaarba.org**, en el caso de Argentina).



Figura 19. El sitio **Protección Online** (**www.protecciononline.com**) cuenta con una serie de consejos sobre la temática de menores en Internet.

Las **recomendaciones** que se dan normalmente para los **educadores** son, en líneas generales, las **mismas** que se aplican a los **padres**, tal como indicamos en el **Capítulo 5**, por lo que es importante que los docentes también las conozcan.

Debemos tener en cuenta también que en **cada etapa** escolar los niños tendrán **distintos intereses**, por lo que es importante consultarlos y conocerlos desde el propio diálogo con ellos. De hecho, esa sería la manera más segura y directa de comprender los hábitos de los niños: logrando el intercambio de ideas entre ellos, discutiendo el uso que le dan a cada cosa, cómo lo hacen, por qué y para qué.

Para el caso de los docentes que siempre tienen estudiantes de la **misma edad**, es importante destacar que, por más que cada etapa de crecimiento y desarrollo está signada por las mismas reglas biológicas y socioculturales, los tiempos **cambian** demasiado rápido como para considerar tan libremente que podemos aplicar las mismas precauciones **de un año a otro**. Por lo tanto, es recomendable **mantenerse actualizados** en cuanto al uso que hacen los menores de las tecnologías año a año. Un buen nivel de actualización y una **cercanía personal con las tecnologías** pueden sumar mucho al rol de educadores.



Figura 20. El portal educativo del estado argentino **educ.ar** (**www.educ.ar**) es una gran fuente de información para el uso de tecnologías en el aula.

También es menester hablar sobre los **riesgos** de la tecnología y el uso de Internet en las **reuniones de padres**, dada la importancia de que las reglas y principios generales que se tomen para hacer cumplir estén lo más **alineados** posible entre **la casa y la escuela**. Esto podría además **alertar** a muchos padres que no estaban al tanto de la problemática o aprovechar a quienes están en el tema y quieran ofrecer ideas, **recomendaciones**, consejos o soluciones que hayan implementado en sus propias familias. Este intercambio de experiencias puede ser muy productivo para docentes y padres.

Si con ayuda de algún software que provea la institución educativa se permite **monitorear** las acciones de los alumnos y mantener el control sobre sus acciones, es importante que se **respete su privacidad**. Al final de cuentas, la mejor relación que se puede establecer con un menor está basada en la **confianza** y no en la **autoridad** o la capacidad de **ejercer poder** sobre ellos.

Promover entre ellos la práctica del **respeto mutuo** también es de suma importancia, en especial, para prevenir casos de ciberbullying, que tanto pueden afectar la integridad y minar la autoestima de los menores. De la misma manera, explicarles la importancia del **trato online** en relación al **trato personal** es otro paso importante en el camino de las buenas prácticas.



Figura 21. Aunque en muchos casos es difícil tratar a los alumnos en forma personalizada, esto produce excelentes resultados.

Para el caso de los más pequeños, **menores a 4 años**, pese a su limitada capacidad de atención, pueden comenzar a **incorporar experiencias** en Internet que permitan **estimular sus capacidades**, sus habilidades de **motricidad fina** con las manos y el arma más poderosa de esa edad: **la imaginación**.

Cuando las escuelas o las instituciones a las que el docente está vinculado no cuenten con una **política formal** de uso de la tecnología o no consideren en sus normas los riesgos asociados a su uso, es bueno **poner en tema a las autoridades** y a otros docentes, para que entre todos contribuyan al bienestar y la seguridad online de los niños.

Sabemos que **la escuela** es el entorno que definirá en mayor medida **la vida** de los niños; por consiguiente, todo lo que podamos **enseñarles** y **transmitirles** durante ese período quedará grabado con la firmeza que solo el tiempo puede demostrar. Y por sobre todas las cosas, no debemos olvidar nunca que la mejor forma de enseñar es **a través del ejemplo**.



RESUMEN

En este capítulo hemos analizado las problemáticas de la tecnología utilizada por los menores desde la perspectiva del educador, que muchas veces enfrenta complejos desafíos y situaciones específicas en el trato cotidiano con sus estudiantes. En ese sentido, describimos el uso de distintas tecnologías de la información en entornos educativos, analizamos el panorama actual de los centros de enseñanza y estudiamos algunas tecnologías educativas que serán herramientas cada vez más comunes en las aulas y fuera de ellas. Por último, listamos una serie de recomendaciones orientadas especialmente al docente.

Actividades

TEST DE AUTOEVALUACIÓN

1. Determine qué elementos tecnológicos se encuentran en el propio entorno educativo (escuela, colegio, instituto, etcétera) y no están siendo aprovechados por completo.
2. Suscríbase a un curso online (MMOC) orientado a docentes, tanto para conocer el tipo de plataforma como para encontrar nuevos focos de información y capacitación profesional.
3. Identifique las oportunidades de mejora que encuentra en los contextos educativos en que se desempeña, en relación al uso de la tecnología en el aula.
4. Analice el uso que le da a las redes sociales y conéctese con especialistas y comunidades relacionadas con la educación. En caso de que no las utilice, cree un perfil personal en alguna de ellas para comenzar a interactuar.
5. Comparta los consejos y recomendaciones que le resultaron de mayor utilidad con otros docentes que no estén familiarizados con la problemática.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:
profesor@redusers.com

*07

Un marco jurídico adecuado

En este capítulo veremos el estado de la legislación actual en temas relacionados con Internet y los menores, definiremos qué cosas son y no son ilegales, y describiremos el camino hacia un marco jurídico que pueda contener las problemáticas actuales como la piratería y otras actividades online, que suelen ser tema de discusión.

- Tecnología y leyes 150
- Nuevas necesidades 154
- Legislación internacional 159
- Leyes en Latinoamérica 164
- Leyes en Argentina 166
- Resumen 171
- Actividades 172

Tecnología y leyes

En un **Estado de derecho** que se precie de tal, las leyes relacionadas con la tecnología no podrían quedar fuera del juego, pero alcanzar un nivel estable donde la **continua evolución** esté reglamentada y acorde con el desarrollo tecnológico es poco más que una **utopía** a la que difícilmente nos acerquemos por mucho tiempo. Dependiendo del **sector** al que se refiera, el sistema legal avanza a una velocidad diferente. No es lo mismo legislar sobre el **fraude**, la **violencia** y el **comercio exterior** que sobre **tecnología**, dado que esta última evoluciona a un ritmo **difícil de seguir**. Por su parte, la sociedad se adapta con velocidad a la tecnología, modificando en base a ella hasta su manera de relacionarse, de trabajar y de convivir.

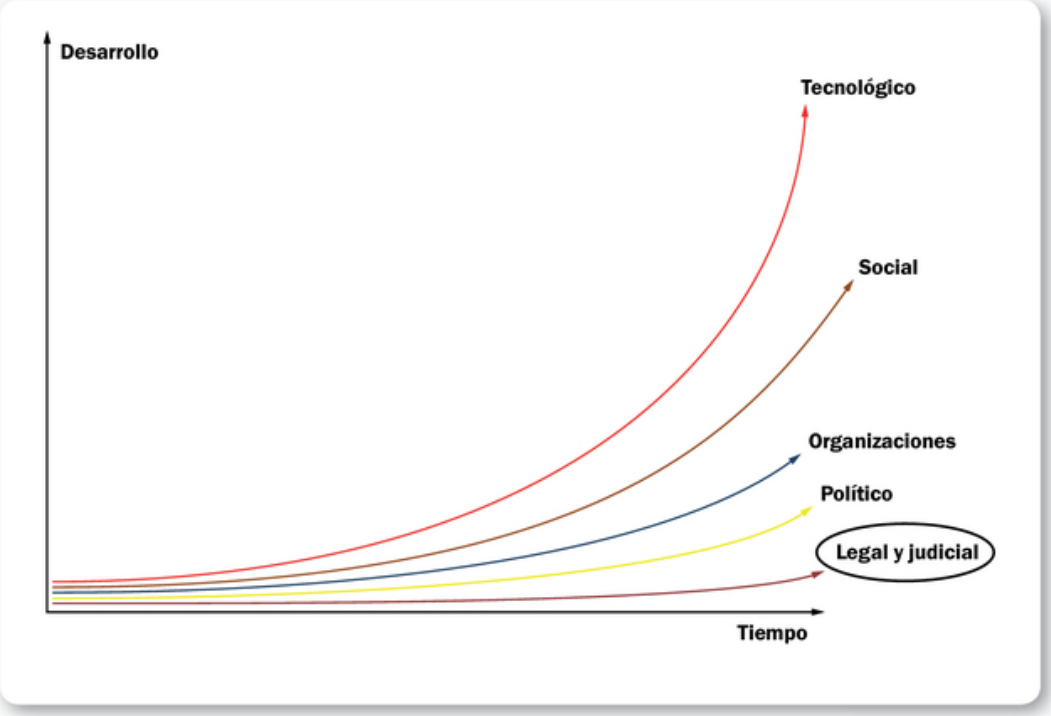


Figura 1. El avance de la legislación frente a la tecnología es mucho más lento y gradual que en otros ámbitos. Fuente: `www.informaticalegal.com.ar`.

En una legislación ideal deberíamos estar protegidos, por ejemplo, contra el **robo de identidad** (**física** y **virtual**). Por otro lado, la vinculación del Estado con las empresas tendría que permitir la existencia de **canales abiertos** y formales para el acceso a la

información que se requiera en casos de investigación. También deberíamos estar protegidos contra toda clase de **abuso a menores**, desde la violencia **física y sexual** hasta la violencia **psicológica y emocional**, difíciles de demostrar pese a las profundas secuelas que pueden dejar. Esta protección debería considerar todo tipo de comunicación y contacto para garantizar que el **grooming** esté incluido, así como también condenar la acción preparatoria a un **potencial encuentro** con menores, de manera que las fuerzas policiales tengan la posibilidad de actuar **de forma preventiva**.



Figura 2. En la actualidad, la rama llamada **Derecho Informático** está teniendo grandes avances.

De la misma manera, la legislación ideal debería penar fuertemente la producción, la distribución y la comercialización de **pornografía infantil** (algo que de hecho hace) y dotar de suficientes atribuciones a las fuerzas policiales para que puedan investigar sospechosos **sin tantas restricciones** (cosa que en muchos casos no consiguen). Esto último no es un caso aislado, por que gran cantidad de veces el problema no se encuentra en la ley sino **en la forma en la que se aplica**, ya que con el objetivo de sostener las **garantías constitucionales** tiende a proteger a los delincuentes de la misma manera que a cualquier otro ciudadano. Esto conforma una especie de **paradoja** difícil de resolver, ya que si

una persona tiene derecho a la privacidad, toda persona debería tenerlo, sin importar su actividad, raza o credo. Por otro lado, los procesos judiciales suelen ser monumentos a la **burocracia** en casi todos los países del mundo, y es esta cualidad la que a veces limita el accionar de la policía, su **brazo operativo**.



Figura 3. Es importante dotar a las fuerzas de seguridad con tecnologías acordes con las problemáticas que enfrentan.

Por ejemplo, si se detecta que un menor está secuestrado, que es víctima de **grooming** o engaño, y se tiene identificada la ubicación del secuestrador con **métodos técnicos**, como la **geolocalización** a partir de una foto o la **triangulación** de llamadas a celulares, es necesario obtener la orden de un **juez** para que se permita realizar un **allanamiento** del lugar donde se cree que se encuentra el menor

LÍMITES DE LA LEY

Muchos esperan que la ley contemple temas como la privacidad, sin pensar que en primera medida son responsabilidad personal, y el hecho de dar a conocer acciones privadas y datos, en otra época impensado, es en sí un riesgo. Por tanto, no es correcto esperar que una política de confidencialidad de un sitio o una ley nos protejan, sino que debemos hacernos más concientes de la información que proporcionamos.

o alguna pista que lleve hacia él. Tal procedimiento, que podría demorar **algunas horas**, es más que suficiente para que el delincuente cambie su ubicación y que sea difícil encontrarlo. Esto denota en sí mismo una **limitación en el sistema**.



Figura 4. La tecnología informática ha traído la necesidad de peritos especializados para asesorar a los jueces.

En efecto, el derecho en su concepción de **ordenamiento**, que establece mínimos de **convivencia social**, con normas aplicables a territorios delimitados, donde el incumplimiento es sancionado por sus normas aplicables, **no es suficiente** en los tiempos que corren.

> LA PROTECCIÓN DE LOS DATOS PERSONALES DEBE SER PARTE DE TODO SISTEMA JURÍDICO

Un gran avance de los últimos años se ha dado en la **tipificación** del delito de **pornografía infantil por medios electrónicos**, pero muchos otros temas no han sido aún alcanzados.

Otra de las leyes que debería contener todo sistema jurídico es aquella que proteja los datos personales, lo que se conoce como **hábeas data**. Esto implica el derecho de cualquier persona que figure en una **base de datos** de acceder a ese registro para conocer la información que contiene sobre sí misma y exigir la **corrección** o **eliminación** en caso de que le

cause algún tipo de perjuicio. Su objetivo es garantizar el **derecho al honor**, la **intimidad** y el acceso a la información personal registrada, y se aplica tanto a personas físicas como jurídicas.

En cuanto a los temas relacionados con la **propiedad intelectual**, es necesario que existan regulaciones al respecto. En las últimas décadas, las leyes de propiedad intelectual se han hecho extensivas para incluir otro tipo de obras del intelecto humano, como el **software**.



Figura 5. Muchas veces, detener a un delincuente implica procedimientos más complejos de lo que parece.

Nuevas necesidades

En cuanto a la piratería y los contenidos ilegales, es probable que las **respuestas** a estas cuestiones no provengan exclusivamente del **ámbito legal** sino que requieran el abordaje desde un **replanteo de la industria** de los medios que alcance la educación y concientización en el consumo y en la generación de contenidos, buscando converger en **soluciones integrales**. En efecto, será necesario **educar** a las nuevas generaciones para que comprendan que vivirán en un mundo en el que **producir contenidos** estará sujeto a las **reglas implícitas** que se han escrito antes de que ellos pudieran interactuar con la realidad.



Figura 6. Los problemas de generación y distribución de contenidos ilegales son demasiado radicales y solo pueden resolverse desde la educación.

Gran cantidad de empresas se han adaptado a los tiempos con bastante **realismo** y **expectativas**, lo que las ha llevado en muchos casos a cambiar sus planes, su **modelo de negocios** y el modo en que se vinculan con sus **clientes**. Así, por ejemplo, muchas productoras de cine y televisión ponen a disposición **parte de sus contenidos** para que sean accedidos oficialmente. De esta forma, **no es necesario piratear** el contenido mediante una grabación del video en el momento de su emisión, ya que se ofrece directamente **sin intermediarios**, quizás con alguna modificación, como publicidad adicional, tiempo de demora en estar en línea, etcétera. Asimismo, muchas señales cuentan con un canal de **YouTube** desde donde amplifican su **distribución**.

¿COPIAS LEGALES?

En cuanto a los contenidos de audio y video, es importante mencionar que lo que prohíbe la ley no es la copia en sí misma, ya que esta puede ser utilizada para uso personal, sino pasar desde CD a formato MP3 para llevar los archivos en un reproductor, copiar un MP3 bajado legalmente a distintos reproductores o copiar un DVD o Blu-ray para proteger al original del desgaste dado por el normal uso.



Figura 7. En un futuro no muy lejano, nuestras identidades física y virtual estarán cada vez más emparentadas legalmente.

Otra de las acciones que están prohibidas por ley es la **extracción** de un video de un sitio de **streaming**, como **YouTube** o **Vimeo**, para que quede almacenado en un archivo de la computadora y no requiera que vuelva a transmitirse para reproducirlo. Al acto de transformar un **CD** a archivos de audio, el de extraer el sonido de un video o el de bajar un contenido que se está transmitiendo online se lo conoce como **rippear**.

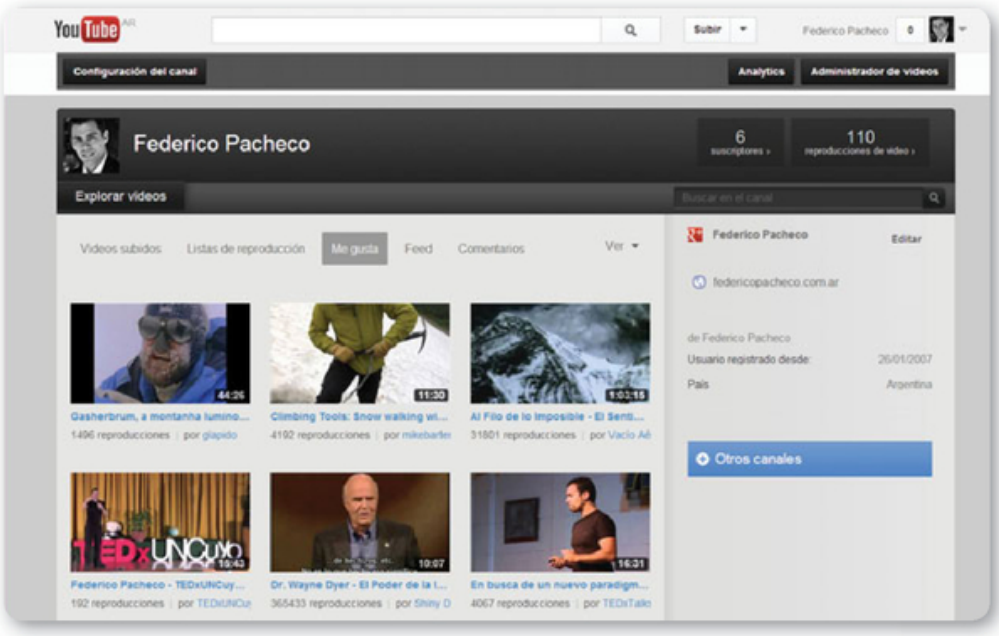


Figura 8. YouTube no permite descargar contenido sin un enlace oficial.

En lo que concierne a la privacidad, y considerando que los conceptos de **esfera íntima** y **privacidad** se han visto modificados en los últimos años, nos hemos encontrado con una nueva realidad que todavía no es fácil de encarar. Si bien el intento de controlar la tecnología utilizando la misma tecnología puede resultar ridículo, debemos reconocer que a este estado hemos llegado por **nuestras propias acciones**.

Uno de los conceptos más discutidos en ámbitos académicos y legales es el del llamado **derecho al olvido**, que implica la facultad de **eliminar información** considerada obsoleta debido al tiempo transcurrido, que se presupone que ya ha perdido relevancia. Esto, sin embargo, no existe como tal en el contexto de Internet y se cree poco probable que pueda ser instrumentado en el corto y mediano plazo.



Figura 9. **Blockbuster**, la cadena de videoclubes más grande del mundo, pagó con la quiebra las consecuencias de la piratería.

EL FIN DE BLOCKBUSTER

Blockbuster Inc., la cadena de videoclubes más grande del mundo, se declaró en quiebra en septiembre de 2010. Tal como puede suponerse, la empresa no logró adaptarse a un mercado virtual que ofrece contenidos digitales, tanto legal como ilegalmente, habiendo encontrado en la piratería su estocada final. Esto repercutió en todos los países con filiales e impactó en la vida de muchas personas.

Tal vez el abordaje más integral sobre temas relacionados al cibercrimen es el dispuesto en el **Convenio sobre Cibercriminalidad de Budapest** (*The Convention on Cybercrime*), ya que es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y le da tratamiento de carácter prioritario a una política penal contra la ciberdelincuencia. Este convenio fue adoptado por el **Comité de Ministros del Consejo de Europa** en el año 2001, se firmó en Budapest el mismo año y entró en vigencia en 2004. Su objetivo es **armonizar las legislaciones** en los Estados miembros de la Unión Europea y está abierto a países como Australia, Japón, Canadá, Sudáfrica y Estados Unidos, aunque otros países interesados pueden **solicitar invitación para su adhesión**. De esta manera, este convenio internacional intenta funcionar como plexo jurídico para los delitos informáticos y el cibercrimen.



Figura 10. El Consejo de Europa firmó el Convenio sobre Cibercriminalidad en el año 2001 en Budapest.

De cualquier forma, si consideramos que las leyes obedecen a los **usos y costumbres**, está claro que los usos y las costumbres están cambiando, de manera que leyes escritas hace tan solo algunas décadas ya pueden parecernos **obsoletas**.

Legislación internacional

La **Organización de las Naciones Unidas** (**ONU**) ha señalado con certeza que cuando los problemas llegan al **ámbito internacional**, se amplifica su magnitud, algo que puede verse claramente con los delitos informáticos. Esta organización propone una **segmentación taxativa** respecto a qué considerar como delito informático:

- **Fraudes cometidos por manipulación de computadoras**, que incluye la manipulación de datos de entrada o salida, de programas, y el fraude a partir del mal manejo de sistemas informáticos.
- **Modificación de datos de entrada**, que abarca la manipulación con el objeto de modificar datos almacenados en un equipo y la falsificación de documentos comerciales.
- **Modificaciones de programas o datos digitalizados**, que contempla el sabotaje informático, el acceso no autorizado a servicios y sistemas y la reproducción no autorizada de software que se encuentra protegido.

Además de la tipificación propuesta por la ONU, el **XV Congreso Internacional de Derecho**, realizado en **Río de Janeiro** (**Brasil**) en 1994, ha propuesto todas las formas de **conductas lesivas** de las que puede ser objeto la información. Estas son: **fraude** informático, **falsificación** en materia informática, **sabotaje** y daños a datos o software, **acceso no autorizado**, **intercepción** de información sin autorización, reproducción no autorizada de software protegido, **espionaje** informático, uso no autorizado de un equipo, **tráfico de claves** obtenidas ilícitamente y distribución de código malicioso (**malware**).



Figura 11. Con la llegada de las nuevas tecnologías, muchos delitos debieron ser ampliados para abarcarlas.

Dado que los contenidos ilegales están vinculados a **grandes mercados** de consumo masivo, este es uno de los temas que más rápidamente se han tratado en el mundo, incluso mucho antes que los relacionados al abuso infantil. Así, **muchos países** han modificado sus antiguas leyes para incluir penalizaciones sobre la violación de los derechos de autor en **forma digital**, aunque las **soluciones** en todos los casos han sido **parciales**.



Figura 12. El cibercrimen se relaciona con el uso de la tecnología para cometer delitos.

Por ejemplo, **España** cuenta desde hace algunos años con lo que se dio en llamar **canon digital**, que implica el cobro de un valor adicional por la compra de ciertos dispositivos electrónicos en **compensación** a los autores por las descargas ilegales. **Francia**, por su lado, castiga

LOS MÁS EXPERIMENTADOS

En 1986, **Alemania** reformó su código penal para contemplar algunos delitos como **espionaje de datos**, **estafa informática** y **falsificación de datos probatorios**, convirtiéndose en uno de los países con más larga data en la aplicación de leyes relacionadas. **España** también fue un país adelantado, ya que cuenta desde 1999 con una **Ley Orgánica de Protección de Datos** (**LOPD**) de carácter personal.

con el corte de la conectividad al detectarse descargas ilegales, bajo la ley conocida como **Hadopi**. También **Inglaterra** posee una ley similar. Pese a los esfuerzos de dichos países, la experiencia demostró que las medidas no fueron del todo efectivas.

Por su parte, **Estados Unidos** tomó una controvertida medida legal al presentar en octubre de 2011 la ley **SOPA** (por su sigla en inglés, **Stop Online Piracy Act**) con el objetivo de intentar controlar las **descargas online**. Previamente, ese mismo año, ya se había presentado un proyecto relacionado llamado **PIPA** (**Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act**), que tenía como fin declarado el de brindar al Gobierno norteamericano y a los titulares de los derechos de autor un conjunto de medios que permitirían **limitar el acceso** a sitios web que infringieran sus leyes, incluyendo los registrados fuera de su territorio.

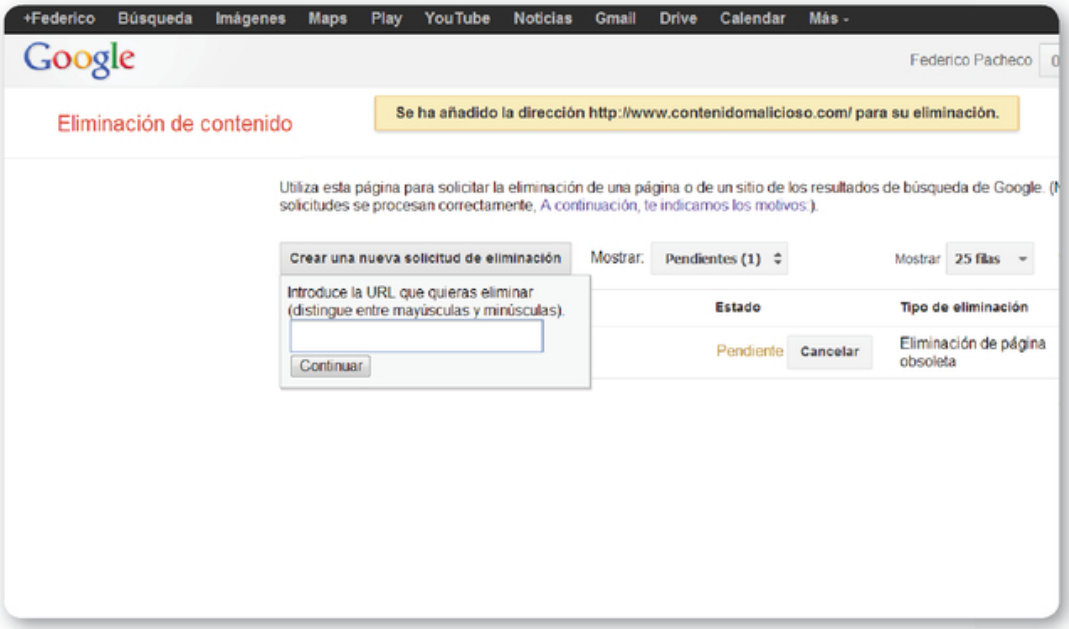


Figura 13. Google ofrece una herramienta para denunciar sitios con contenido difamatorio.

Más allá de SOPA y PIPA, Estados Unidos contaba ya con una ley federal sobre derechos de autor bastante controversial llamada **DMCA** (**Digital Millennium Copyright Act**), que sanciona las infracciones en la reproducción y la producción y distribución de cualquier tecnología que facilite a una persona evitar las medidas de protección de **contenidos digitales** (llamadas **DRM** o **Digital**

Rights Management). También aumenta las penas para las infracciones al derecho de autor en Internet.

En cuanto al **grooming**, debido a lo delicado del tema, muchos países han avanzado rápidamente al respecto. En ese sentido, la **Convención sobre cibercriminalidad** del **Consejo de Europa** se ocupó del tema en su informe **Protection of Children Against Abuse Through New Technologies**, que ya consideraba a la pornografía infantil en Internet. No obstante, algunos países no han incluido referencia al **grooming** en sus legislaciones.



Figura 14. Muchos sitios como Wikipedia se unieron a la protesta por las leyes SOPA y PIPA.

España, por ejemplo, tuvo en 2010 una reforma en el código penal que le permite penalizar la **captación de menores** por Internet con fines sexuales, y además considera **agresión sexual** los actos que

DMCA Y LA CONTROVERSIA

Electronic Frontier Foundation (EFF), organización destinada a preservar los derechos de libertad de expresión, se ha manifestado abiertamente contra los efectos de las medidas de DMCA. Según explica la EFF, esta ley limita la libertad de expresión y la investigación científica, además de poner en peligro el uso legítimo de la tecnología, impidiendo así la competencia y la innovación.

atenten contra la libertad e indemnidad sexual en caso de que la víctima sea **menor de edad**, a pesar de que no haya violencia ni intimidación.

En **Alemania** se prohíbe el ejercicio de influencia sobre un menor por medio de la exhibición de pornografía o conversaciones en tal sentido.

En **Inglaterra**, ya desde 2003, el **Sexual Offences Act** pena el **encuentro** o la **organización** de encuentros con menores, para uno mismo o terceros, con **intención** de abuso sexual. En el mismo Reino Unido, **Escocia** introdujo en 2005 una idea similar en la **Protection of Children and Prevention of Sexual Offences Act**. Estas últimas cuentan con la ventaja de que pueda considerarse un delito la intención misma sin haber llegado a realizarse el encuentro físico.

> MUCHOS PAÍSES ESTÁN CREANDO LEYES PARA PROTEGER A LOS MENORES DE EDAD

En el caso de **Australia**, por ejemplo, hay penas de hasta 15 años de prisión para todo aquel que haga uso de servicios de telecomunicaciones para involucrar, alentar o reclutar a menores de 18 años en actividades de **índole sexual**, y ya en 1995 el **Criminal Code Act** prohibía el uso de tales servicios para contactar menores de 16 años o exponerlos a **material indecente**.



Figura 15. La Agencia Española de Protección de Datos vela por el cumplimiento de la legislación sobre protección de datos personales en España.

En **Estados Unidos** también está prohibida la **comunicación** con menores de 18 años con el fin de cometer abuso sexual, en tanto que algunos estados (como el caso de **Florida**) cuentan con **disposiciones adicionales**. De manera similar, en **Canadá**, el **Criminal Code** condena la comunicación con menores con fines sexuales por medio de sistemas informáticos.

Leyes en Latinoamérica

América Latina, como ocurre en muchas otras ocasiones, **camina algunos pasos por detrás** de los países más desarrollados. Pese a esto, con el tiempo se ha ido adaptando y en la actualidad, está haciendo un gran esfuerzo por ponerse a la altura de las legislaciones más avanzadas. Por ejemplo, respecto a los delitos informáticos, Chile (1993), Venezuela (2001), Argentina (2008), Colombia (2009), Bolivia (2011) y México (2012) tienen leyes específicas relacionadas con el tema.

Algunos casos merecen mención específica, como **Chile**, que ha sido pionero en lo referido específicamente al **grooming** y tiene en vigencia un cuerpo normativo que pena al que por cualquier medio (incluyendo informático) realiza actos de **acoso a menores** de edad con el objeto de recoger **imágenes** o información de carácter personal de ellos, o lograr actividades de **índole sexual**. Además, este país cuenta con una Ley de delitos informáticos (1993), leyes de firma electrónica, neutralidad en la red y otras relacionadas con el derecho informático.

Colombia posee además leyes específicas para el comercio electrónico y el gobierno electrónico, entre otras más comunes. **Venezuela**, por su lado, ha dictado una serie de decretos orientados a

FOCO EN EL GROOMING EN ESTADOS UNIDOS

El país del norte tuvo un caso muy resonante en el año 2009, que fue el de Jerry Alan Penton, de Alabama. Fue el primer sentenciado por cometer el delito de grooming propiamente dicho. Penton recibió la pena de 20 años de prisión por sus acciones relacionadas con el abuso de menores, más otros 20 años por distribución y posesión de pornografía infantil.

regular distintos aspectos del derecho informático, y es de destacar el caso de **Uruguay**, que dispone de un amplio plexo legal.



Figura 16. Muchos países de Latinoamérica han adaptado rápidamente sus legislaciones, como el caso de Brasil.

En cuanto a la protección de datos personales, una veintena de países cuentan con legislación al respecto. Algunos han **modificado su constitución** para contemplar el concepto, como, por ejemplo, **Brasil**, que fue el primer país del mundo en incorporarla a su constitución en 1988, seguido en Latinoamérica por **Colombia** en 1991, **Paraguay** en 1992, **Perú** en 1993, **Argentina** en 1994 y **Ecuador** en 1996. Posteriormente, fue incluida por **Venezuela** (1999) y **República Dominicana** (2010). Otros países, además de contemplarla en su constitución nacional, tienen **leyes específicas** de hábeas data, como **Bolivia** (2004), **Chile** (2002), **México** (2007), **Nicaragua**, **Panamá** (2002), **Uruguay** (2008) y **Guatemala** (2008).

CHILE, PIONERO EN COMBATIR EL GROOMING

Chile cuenta con un caso modelo en la penalización del grooming. En 2008, un hombre de 26 años, que mantenía una amistad con su vecina de 13 por mensajería instantánea, la motivó a posar desnuda frente a su webcam y luego, utilizó las imágenes para extorsionarla. El acosador fue condenado a cinco años y medio de privación de la libertad tras el proceso penal.

De esta manera, América Latina ha intentado avanzar para mantenerse a la par de otros sistemas jurídicos y **poder alinearse** con los más altos estándares a nivel internacional.

Leyes en Argentina

La legislación argentina ha suscrito diversos **tratados internacionales** que le permitieron avanzar en materia de legislación informática, convirtiéndola en una de las más avanzadas de Latinoamérica. Uno de ellos fue el acuerdo celebrado en el marco de la **Ronda Uruguay del Acuerdo General de Aranceles Aduaneros y Comercio**, que establece que el software sería protegido como obra literaria en conformidad con el **Convenio de Berna** para la **Protección de Obras Literarias y Artísticas** (1971). Así se determina que toda compilación de datos legible podrá ser protegida como una creación de carácter intelectual. Además, para casos de falsificación dolosa de marcas de fábrica o de **violación del derecho de autor a escala comercial**, se establecerían sanciones penales.



Figura 17. El código fuente de un programa es considerado una obra que puede ser sujeta a propiedad intelectual.

MÁS TRATADOS

Otros tratados suscritos por la Argentina fueron la Convención sobre Propiedad Intelectual de Estocolmo (1967) en 1980 y el Convenio de Berna en 1990, y se ratificaron la Convención para Protección y Producción de Fonogramas (1971) en 1972 y la Convención Relativa a Distribución de Programas y Señales en 1994. Hay otros convenios no ratificados en la OMPI (Organización Mundial de la Propiedad Intelectual) de la que el país es parte desde 1980.

El resultado más directo de estos tratados ha sido la Ley 25.036, que modifica la Ley 11.723 o **Ley de Propiedad Intelectual**, para incluir el **código fuente** y **objeto** de un programa como creación susceptible de ser protegida por los **derechos de autor**.

Por otra parte, el país cuenta con la Ley 24.766 o **Ley de Confidencialidad** (1997), que protege datos a través de acciones penales y civiles, sancionando con la pena de **violación de secreto** la sustracción de medios de almacenamiento y el acceso sin autorización a una red o computadora que contenga información confidencial. Esta considera como **información confidencial** aquella que tiene las siguientes características:

- **Es secreta** en el sentido de no ser generalmente conocida ni de fácil acceso para personas de círculos en los que se utiliza con normalidad.
- **Tiene valor comercial** por el hecho de ser secreta.
- Existen **medidas** implementadas para **mantenerla secreta**.



Figura 18. En base a las leyes modernas, es posible ser condenado a prisión por actividades relacionadas con la ciberdelincuencia.

Otra ley relacionada con la tecnología informática es la Ley 25.326 o **Ley de Protección de Datos Personales** o **de Hábeas Data** (2001), que además de contemplar el concepto legal de hábeas data define un organismo de control sobre su aplicación, que supervisa el tratamiento por parte de empresas e instituciones públicas y exige a toda organización una declaración de las **bases de datos** con las

que cuente para generar **transparencia** sobre su existencia. Además, define los **datos personales** y un subconjunto llamado **datos sensibles**, que son aquellos que revelan información que podría ser utilizada para ejercer **discriminación** sobre una persona, como el origen racial y étnico, las opiniones políticas, las convicciones religiosas, filosóficas o morales, la afiliación sindical y la información referente a la salud o a la vida sexual. Dicha ley determina que **nadie puede ser obligado a proporcionar datos sensibles** y que estos solo pueden ser recolectados y tratados por razones autorizadas por ley.



Figura 19. La Dirección Nacional de Protección de Datos Personales es el órgano de control de la Ley de Hábeas Data en la Argentina.

Durante el mismo año entró en vigencia la Ley 25.506 o **Ley de Firma Digital**, que reconoce la validez legal de la firma digital, concebida como un conjunto de **algoritmos criptográficos** y

PIONEROS EN EL MUNDO

En 1976, el FBI dictó el primer curso de entrenamiento sobre delitos informáticos para sus agentes. En 1986, se dictó la **Computer Fraud and Abuse Act**, que hace referencia a delitos de abuso o fraude contra instituciones financieras y registros médicos. También especificaba penas para el tráfico de claves con la intención de cometer fraude y declaraba ilegal el uso de contraseñas de forma inadecuada.

no como una firma hológrafa digitalizada. Además, regula la creación, la utilización y los alcances de la firma digital y el documento electrónico, y crea un **ente administrador** para otorgar las licencias habilitantes para acreditar a los certificadores en las condiciones fijadas por la ley.

Si bien no ha tenido gran repercusión, esta ley permitiría que cualquier ciudadano cuente con un mecanismo de **autenticación personal**, lo que evitaría que pueda ser vulnerada la demostración de su identidad.



Figura 20. La firma digital no implica la digitalización de la firma manuscrita, sino un procedimiento técnico sobre los documentos.

El último gran paso en relación con las tecnologías de la información vinculadas a la seguridad lo dio la Ley 26.388 o **Ley de Delitos Informáticos** (2008), que modifica el Código Penal para incluir **nuevos tipos penales** y sus respectivas penas. Esta ley **generó gran**

PIRATERÍA EN LA INDUSTRIA AUDIOVISUAL

La industria audiovisual argentina se ha visto afectada en el año 2009 por el cierre de empresas tradicionales, como Gativideo y LK-Tel, editoras con trayectoria de más de dos décadas. Esto fue resultado de la caída de casi el 50% en ventas durante su último año y del 70% en los últimos tres. En la misma oleada, más de 2.500 videoclubes cerraron en Argentina entre 2008 y 2011.

controversia en algunos puntos por los **vacíos** que deja y además, no se ha logrado aún llevar al nivel de procesos y procedimientos, ni dotar en general a las **fuerzas de seguridad** e investigación de los medios técnicos para investigar, recolectar y presentar pruebas, con lo cual en cierto punto podría considerarse incompleta hasta la fecha. No obstante, estableció las bases legales para comenzar a actuar en casos en donde hasta este momento era imposible incursionar o debían acomodarse para que encuadraran dentro de un delito tipificado. Entre los delitos contemplados se encuentran:

- **Distribución** y **tenencia** de **pornografía infantil** con fines de distribución.
- Violación de **correo electrónico**.
- **Acceso ilegítimo** a sistemas informáticos.
- Daño informático y distribución de **virus**.
- **Daño informático** agravado.
- **Interrupción** de comunicaciones.



BOLETIN OFICIAL
DE LA REPUBLICA ARGENTINA

Buenos Aires, miércoles 25 de junio de 2008
Año CXVI
Número 31.433
Precio $ 0,80

Primera Sección
Legislación y Avisos Oficiales

Sumario

Pág.

LEYES

CODIGO PENAL
26.388
Modificación. 1

PARQUES NACIONALES
26.389
Modificación de la Ley Nº 22.351. 3

PROHIBICION DEL TRABAJO INFANTIL Y PROTECCION DEL TRABAJO ADOLESCENTE
26.390
Modificación de las Leyes Nº 20.744, 22.248, 23.551, 25.013 y del Decreto Ley Nº 326/56. 3

DECRETOS

LEYES

CODIGO PENAL
Ley 26.388
Modificación.
Sancionada: Junio 4 de 2008
Promulgada de Hecho: Junio 24 de 2008

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de
Ley:

ARTICULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

Figura 21. Extracto del Boletín Oficial de la Argentina del día miércoles 25 de junio de 2008, donde aparece publicada la **`Ley de delitos informáticos`**.

Pese a los grandes avances de la legislación argentina, no se cuenta aún con algunos **tipos penales** específicos como el **grooming** o el **robo de identidad**, lo que aumenta la dificultad de castigar estas **conductas** de forma específica. No obstante, en el Congreso Nacional

aguardan su sanción algunos **proyectos relacionados**, en tanto que otros perdieron su estado parlamentario luego de transcurrido el tiempo sin alcanzar su debido tratamiento.



Figura 22. Es importante que se dicten leyes específicas que incluyan las nuevas actividades como el grooming o el robo de identidad.

RESUMEN

En este capítulo hemos visto algunos de los temas referentes a lo legal que son relevantes al hablar de las tecnologías. En general, estos se encuentran desconectados del saber cotidiano y requieren de un especialista en la materia para ser comprendidos. Hemos analizado aquí las nuevas necesidades que aparecen con la tecnología misma, los distintos delitos que deben ser tenidos en cuenta por un sistema jurídico adecuado y la situación actual en distintos países del mundo, incluyendo algunos de Latinoamérica.

Actividades

TEST DE AUTOEVALUACIÓN

1. Hable con un abogado de confianza sobre los temas relacionados con la tecnología para conseguir una mirada profesional al respecto.
2. Averigüe qué proyectos de ley hay en su país o región, relacionados con la seguridad y la tecnología.
3. Investigue si en su país existen antecedentes específicos y casos conocidos sobre grooming.
4. Identifique todos los contenidos que consume que no están correctamente licenciados.
5. Converse con otros padres de familia sobre los temas que le hayan resultado importantes sobre el derecho informático.



PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

*08

Una visión de futuro

En este capítulo final presentaremos un posible cuadro general de la situación por venir, de cara a un futuro que seguro traerá muchos cambios. Finalizaremos con el análisis de una serie de conclusiones relacionadas con el desarrollo y la educación.

- Tiempos de cambio 174
- El camino por recorrer 178
- Desafíos del mañana 181
- Un enfoque integral 185
- Resumen 187
- Actividades 188

Tiempos de cambio

Está claro que estamos atravesando un portal que nos llevará de manera inapelable a una situación de **cambio de época**. Este tipo de transformaciones no se dan con demasiada frecuencia en la historia de las sociedades, pues requieren **cambios de paradigmas**, masas críticas de personas y una **coyuntura particular**, que pocas veces se repite. A los integrantes de la Generación X que analicen el transcurso de su propia vida no les será difícil concluir que las transformaciones se aceleran cada vez más desde los años 70 hasta la actualidad.



Figura 1. **Thomas Kuhn** propuso que los nuevos desarrollos científicos serían examinados a la luz del paradigma presente y raramente ocurriría una revolución que cuestionara el paradigma mismo.

Podríamos decir que uno de los componentes que representan y dan la pauta de que se está en presencia de un cambio de era es, sin lugar a dudas, el **cambio en la visión del mundo** que se tenga como humanidad. Por ejemplo, cuando se pasó del **geocentrismo** al **heliocentrismo** o, como se ha dado en las últimas décadas, de la interpretación física tradicional del universo a la interpretación aportada por la **física cuántica**, con innumerables conclusiones y derivados.

Un cambio de **cosmovisión** impacta fuertemente en todos los órdenes de la vida de las personas, ya que muchas cosas deben ser reinterpretadas y reescritas a la luz de las nuevas formas de concebir la realidad.

GESTIÓN DE LA INCERTIDUMBRE

Las ciencias han contribuido a la adquisición de muchas certezas y, a la vez, nos han revelado grandes áreas de incertidumbre. La educación futura deberá incorporar a la incertidumbre como parte del proceso de aprendizaje e incluir como un hecho el afrontar los riesgos y lo inesperado, en tanto que se pueda cambiar el propio paradigma en virtud del nuevo conocimiento adquirido.



Figura 2. Las decisiones de las personas durante los cambios de época pueden modificar el mundo para siempre.

Otro de los factores que influye en el cambio global y determina que su presencia es ineludible son los **cambios en las instituciones**, desde las figuras y organizaciones religiosas hasta el gobierno, la familia, la universidad o cualquier gran emblema arquetípico en función del cual se sostienen muchos otros conceptos. Cuando las instituciones experimentan embates externos pueden o no sucumbir, pero cuando sufren **roturas internas** e implosiones se está ante la insalvable presencia del principio del fin. Si bien esto no es solo dominio de los últimos años transcurridos, sí se ha intensificado bastante en paralelo a la evolución tecnológica y de las ciencias.

También es un elemento característico la existencia de **tecnologías emergentes**, como fue la rueda, la máquina de vapor, la imprenta, el automóvil, la robótica o las grandes redes. Todo esto permite conformar una **nueva configuración** de la realidad que tiende a organizarse de una manera a veces impredecible y hasta **caótica**, pero que con el tiempo puede comenzar a establecerse y ser interpretada. El problema de este estado emergente es que hasta que pasa un período que lleva a la estabilidad, suele correrse detrás de soluciones temporales que en algunos casos terminan siendo definitivas.

Muchas de estas tecnologías emergentes se reflejaron en la forma en que nos relacionamos. Un interesante estudio realizado por el

especialista en nuevos medios de comunicación, **Thomas Baekdal**, analiza la manera en la que **consumimos la información** durante los últimos dos siglos, destacando el cambio que estos han sufrido en la última década respecto al resto de la historia.

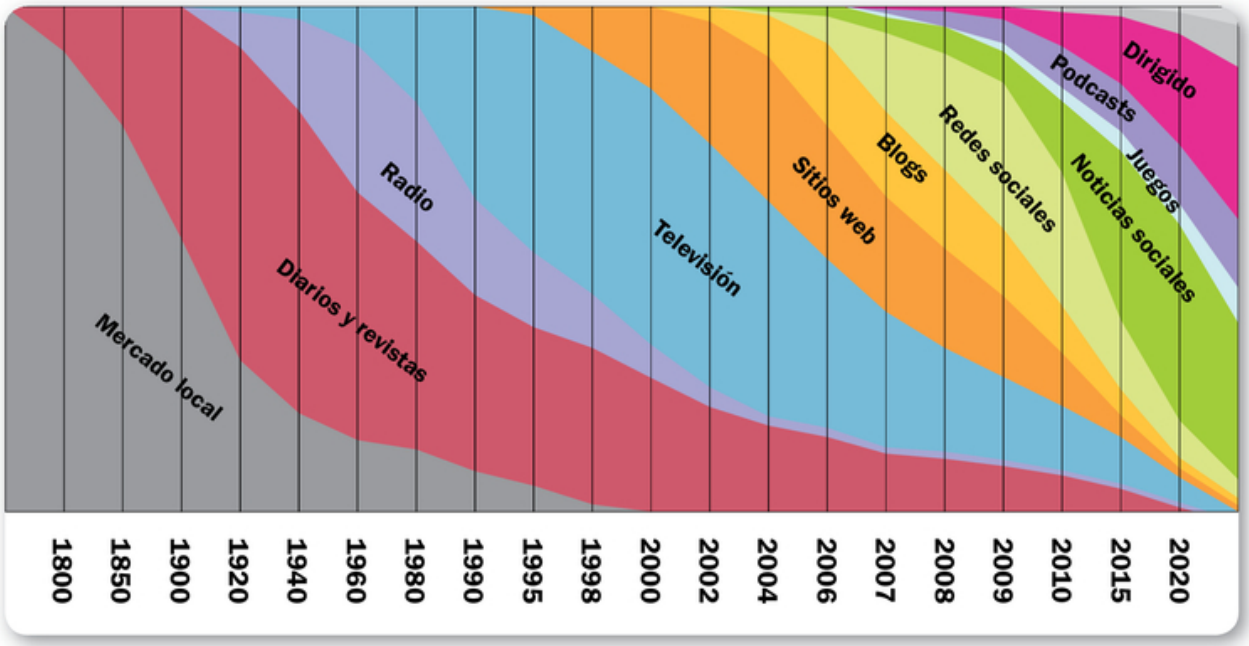


Figura 3. Estudio de Thomas Baekdal sobre la evolución de los medios de comunicación que consumimos a lo largo de la historia.

En un futuro no muy lejano, deberemos estar mejor preparados para no ser **reemplazados** por máquinas o computadoras, algo que aunque pareciera ser una novela trágica de ciencia ficción postapocalíptica, no es más que una parte de la historia que se repite. Así, muchas de las **tareas** que realizan hoy los seres humanos podrán ser efectuadas por sistemas informáticos **inteligentes**, que serán **operados**, **programados** y **creados** por personas. Debido a esto, deberemos agregar un valor especial a nuestra labor para que se justifique nuestra tarea y nuestro rol en el engranaje de la sociedad. Esto, lejos de ser un mal presagio, es un llamamiento a la **conciencia educativa**, por medio de la que debemos conseguir que las personas obtengan más rápido y de manera más eficiente el conocimiento.

> NUESTRA LABOR DEBERÁ TENER UN VALOR ESPECIAL PARA JUSTIFICAR NUESTRO ROL



Figura 4. Muchas funciones básicas que antes realizaban las personas fueron siendo reemplazadas por robots. Aquí, un robot aspiradora.

Adaptarse a la nueva era no será algo trivial para los que hoy son adultos pero sí lo será para los niños, que crecerán al **ritmo de la evolución gradual**, aunque estarán frente a escenarios más complejos que el actual, tratando de adaptarse a **sus propios cambios**.

Es cierto que existe una natural **tendencia** del ser humano a permanecer en la llamada **zona de confort**, para lo que el cerebro ha evolucionado durante millones de años. Esto se debe a la búsqueda del **menor esfuerzo** como forma de adaptación evolutiva y mejora de las posibilidades de **supervivencia**. El problema que esto acarrea es que la **comodidad** en la que estamos en un momento no nos permite avanzar hacia estados más complejos, aunque los **cambios tecnológicos** han forzado al hombre a adaptarse de manera continua para mantenerse.

Tal es la lucha entre nuestra propia naturaleza tendiente a que permanezcamos **estables** y el **caos natural**, que nos obliga a **adaptarnos continuamente**. Esto suele impedir que conozcamos lo que viene, ya que no está al alcance de nuestro horizonte cercano. En suma, más que tratar de **predecir** el futuro, es mejor aprender a **prepararnos** para lo inesperado y estar dispuestos a adaptarnos a las novedades que puedan aparecer.

El camino por recorrer

En este camino que estamos recorriendo nos encontraremos con que en la gran mayoría de los problemas subyace la necesidad de un **enfoque consciente**, más desde lo **humano** que desde lo **técnico**, por lo que la solución fundamental siempre estará basada en la **educación**. A riesgo de parecer reduccionista, hablar de educación no se trata de contar con las **instituciones existentes** para resolver **problemas futuros**, sino de crear nuevas formas de articular el presente para que existan **instituciones adaptadas**, que aprendan al tiempo que enseñan, y que se adapten y evolucionen al ritmo que el mundo lo requiera. Esto suele referirse comúnmente como **organizaciones que aprenden**.



Figura 5. Hay quienes aseguran que los libros en papel tenderán a desaparecer, lo que podría modificar la manera de aprender y enseñar.

Uno de los aspectos en los que mayor foco habrá que poner es en la **legalidad de los contenidos** y la información, ya que la tendencia creciente del consumo de material audiovisual y de textos permite suponer que todavía no se ha encontrado una **solución a la piratería**. La única respuesta aparente es educar a las nuevas generaciones para que conozcan **a priori** la manera en que sus contenidos podrán ser **consumidos** y **multiplicados**, de manera que cualquier modelo de negocios, entretenimiento o distribución futura incluya eso como base y

no sea el veneno de su sistema, como lo ha sido para muchas industrias. **La piratería es repudiable** por donde se la mire, eso está claro, pero ha emergido como respuesta a un mercado de consumo masivo que no pudo adaptarse al ritmo y a las necesidades de las personas sin **limitar sus libertades** para hacerlo.



Figura 6. La piratería se resolverá con educación en producción y consumo de contenidos, en un contexto social y de mercado justo e igualitario.

En esta **línea de razonamiento** podemos arribar a una simple conclusión, considerando que tal como están planteadas las reglas del mundo, si todo siguiera así, sería más probable que se condene a un padre de familia por el uso de un sistema operativo ilegal por el que no está ganando dinero que a una gran corporación que gana millones por permitir que se contamine el medio ambiente con su propia actividad industrial. Esto es, cuanto menos, **paradójico**.



Solo cuando exista **igualdad de oportunidades** reales en el acceso a la información y al consumo de cultura y sus productos relacionados, podremos abordar el tema de su regulación con bases en una **ética sin hipocresía**. El **compartir** es propio de la **naturaleza humana** y restringir esa **libertad** es equivalente a introducir un **cepo social** que permita que se cumplan las reglas por miedo al castigo más que por el propio hecho de lo que esté bien o mal.

Las distintas ciencias nos han mostrado desde diferentes puntos de vista que, sin importar qué aspecto del ser humano analicemos, la forma más segura de evolucionar, progresar y **avanzar** hacia estadios más complejos de **madurez** personal y social es mediante la **interacción** y la **colaboración**. Quizás así se pueda retomar el sentido del viejo refrán: "Si quieres llegar rápido, debes ir solo; si quieres llegar lejos, deber ir acompañado".



Figura 7. Algo que seguro sabemos del mundo futuro es que dependeremos mucho más que nunca unos de los otros para desarrollarnos.

APRENDIZAJE BASADO EN JUEGOS

Dado que el juego siempre ha sido un vehículo de aprendizaje, en especial en la primera infancia, en los últimos tiempos se lo ha estudiado en un sentido pedagógico para que sea incorporable a todas las etapas escolares. En el futuro, el juego podría ser una herramienta educativa más, adaptada en contenidos curriculares para permitir adquirir competencias de manera lúdica y entretenida.

Cualquier incipiente señal de **estancamiento** en un mundo tan dinámico es síntoma de una posible **caída** sobre el propio peso en el corto o mediano plazo. Si miramos los sistemas educativos actuales con cierta perspectiva, es fácil notar que sus bases provienen de al menos **dos siglos atrás** y que no se han modificado demasiado en las últimas décadas, por lo que nos encontramos con un **sistema antiguo** que pretende formar personas nuevas para que se desempeñen en un mundo que aún no se ha creado, y cuyas profesiones y **tareas desconocemos**.



Figura 8. Los sistemas educativos fueron creados bajo necesidades de hace más de dos siglos. De ahí su obligación de evolucionar.

Desafíos del mañana

Resulta dificultoso determinar qué tipo de problemáticas encontrarán las **futuras generaciones** con sus hijos. Seguramente, muchas de las tecnologías que hoy consideramos novedosas estarán ya en su **período de madurez**, por lo que no será inconveniente analizar su **aceptabilidad** o no en los diferentes entornos que ya se habrán transformado en parte de nuestro paisaje.

Según parece, las redes sociales se asentarán como tecnología de base en las **interrelaciones humanas**, vinculando a la gente desde distintos aspectos **complementarios**. Se deberá haber establecido para ese entonces una suerte de **equilibrio dinámico** que permitirá balancear la vida virtual y no virtual, pasado ya el período de explosión sorpresiva y el pico de crecimiento.

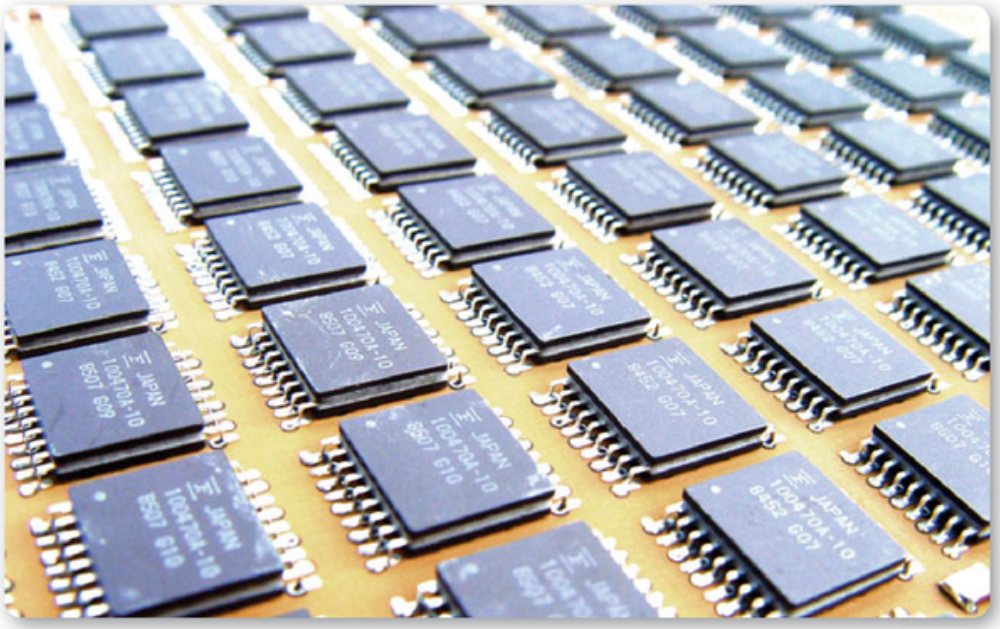


Figura 9. Es realmente cuestionable que la tecnología continúe mejorando la calidad de vida de algunos y aislando a otros.

Es muy posible que al haber cada vez más potencia de cómputo en los **dispositivos móviles**, la cantidad de acciones que realicemos con ellos sea mayor que en la actualidad, y se convirtian en un **par inseparable** para cada persona. Esto llevará a la creación de nuevas medidas de control y protección contra **agentes maliciosos**, pues



EL QUE BUSCA ENCUENTRA

Las tecnologías de los buscadores han avanzado mucho desde su inicio, al punto de contar hoy con la posibilidad de ofrecer sugerencias instantáneas a medida que se escribe, lo que denota una gran potencia de cálculo. Se estima que Google recibe unos 2.500 millones de pedidos de búsqueda por día, y esto lo convierte en el buscador más utilizado del mundo.

vulnerando un dispositivo se podría vulnerar mucho de una persona, además de su **privacidad**. No obstante, los móviles podrán motorizar el acceso ubicuo a la información, alcanzándose una mayor independencia en cuanto al lugar físico.



Figura 10. Los **smartphones** formarán cada vez más parte de nuestras vidas, y llevarán mucha información personal que deberemos cuidar.

Pese a lo descrito, es posible que contar con **más tecnología** no nos brinde más ni mejores soluciones de forma inmediata ni directa si estas no van acompañadas de una conciencia en su uso. Las tecnologías nos proveerán herramientas para resolver **problemas nuevos** y lidiar con los viejos, hasta el punto en que todos podamos **construir herramientas propias** a partir de las que disponemos, independizándonos de un sistema mayor que pueda **limitar nuestras**

CONCIENCIA ECOLÓGICA

Ningún enfoque integral del futuro podría estar completo si no consideramos nuestro entorno y la naturaleza. La ecología y el desarrollo sustentable deberán asentarse como bases para evitar que el mundo continúe siendo destruido por las grandes corporaciones en favor de su beneficio económico y en detrimento de la salud del planeta. Esta conciencia, sin duda, debe partir de la educación.

libertades. De eso se tratará en gran parte el desafío del mañana: **crear creadores y formar formadores**. Lo estático tenderá a desaparecer o colapsar, y seremos testigos de lo que sobreviva al embate evolutivo.

Nada de esto **anula** lo hasta aquí desarrollado. No es que deban demolerse las instituciones ni eliminarse todos los métodos educativos; por el contrario, deberán **reformarse** y **actualizarse** para adaptarse a un mundo mucho **más complejo** que aquel en el que fueron creados. Al fin y al cabo, las **bases biológicas** que rigen las **etapas del aprendizaje** en el ser humano no han cambiado en absoluto, lo que se ha modificado es su **entorno**. A este respecto, no hay muchos avances más que los estudios desarrollados por el biólogo suizo **Jean Piaget** sobre la infancia y las **teorías del desarrollo cognitivo**.



Figura 11. Educar a futuros líderes será uno de los grandes desafíos del mañana.

TECNOLOGÍA Y SALUD

Con el desarrollo de la tecnología, el hombre debió realizar menos esfuerzo físico, lo cual derivó en personas menos saludables, con peores hábitos alimenticios y más sedentarias. Esto, sumado al estrés, los malos hábitos en el uso de la tecnología y las cercanías a fuentes electromagnéticas y radiación, hace que debamos compensar la comodidad del progreso con una mayor conciencia hacia nuestra salud.

Un enfoque integral

Es de esperarse que el futuro de la sociedad esté principalmente en manos de la **educación familiar** que junto a una **educación social** complemente las habilidades necesarias para desarrollarnos como seres humanos y profesionales. En definitiva, la clave del **desarrollo personal** del futuro estará en cómo abordemos las **relaciones interpersonales** y cuánto desarrollemos la **empatía** y otras habilidades propias del **hemisferio derecho** de nuestro cerebro, dejadas de lado por muchos años por las ciencias duras.

La enseñanza de tales **habilidades blandas** no podrá ser meramente teórica, ya que abundan los cursos, clases y materias de derechos humanos, moral y civismo, entre otras. En efecto, estas deberán llevarse a un **nivel vivencial** que se practique a diario y se desarrolle en conjunto con el resto del aprendizaje.

> LA EDUCACIÓN FAMILIAR Y LA SOCIAL COMPLEMENTAN LAS HABILIDADES DE UN SER HUMANO

La naturaleza nos provee los modelos para seguir en casi todos los aspectos, por lo que tal vez deberíamos aprender de otras criaturas del reino animal. Un claro ejemplo son **las hormigas**, que conforman una de las más antiguas especies de la tierra y pese a no haber evolucionado a nivel de su inteligencia, están **sumamente avanzadas a nivel de sociedades**, muy adelantadas a nosotros.

Un enfoque integral de la tecnología, la educación y la sociedad deberá incluir la **libertad personal** en el sentido amplio. Muchos estudiosos concuerdan en que el **control** y las **restricciones** a los ciudadanos impuestos por diferentes **gobiernos** del mundo aumentan, en el largo plazo, la probabilidad de caer en **retrasos económicos y sociales**, lo que puede demostrarse con claros ejemplos. Esto no se trata de una mera opinión subjetiva de unos cuantos sino que se desprende de un análisis en perspectiva de dos siglos de guerras continuas y diferentes formas de gobierno probadas alrededor del globo.

Lamentablemente, hemos visto a través de los siglos que, en su gran mayoría, las tecnologías surgieron como necesidad de **superioridad militar** entre pueblos o países. Así, una **ventaja competitiva** en términos de **armamento** dio históricamente una posición superior de poder a quienes lo creaban y poseían. Esta triste realidad habla

mucho de la naturaleza humana, pero de nosotros depende comenzar a **cambiar el rumbo** de los acontecimientos para que las nuevas tecnologías se creen en favor del **bienestar humano** más que en virtud de la superioridad armamentística o la **carrera científica**.

Por otro lado, la enseñanza deberá hacerse extensiva para alcanzar lo que se comenzó a denominar **educación global**. Esta corriente educativa habla de conceptos fundamentados en **valores universales** como la **solidaridad** y el **respeto mutuo**. Estos deberían ser aprendidos en todo sistema educativo, sin importar el país o la región, de modo que la **base ética** del mundo globalizado también sea común **para todos** los seres humanos.

Sin dudas, las tecnologías acercarán la educación a los **sectores menos beneficiados**, pero las **políticas educativas** y sociales que estén por encima de estas deberán estar **alineadas** con un modelo que realmente busque la igualdad de **oportunidades** y posibilidades de **acceso a los recursos fundamentales**. Con la **eliminación de la desigualdad**, las sociedades se volverán **más pacíficas**, ya que no habrá necesidad de odiarse y comportarse con violencia por el hecho de que otros tengan más que uno, solo por haber nacido en otro contexto. En cierto modo, si la tecnología no sirve para esto, entonces no habrá servido para nada.



Figura 12. La tarea del educador será clave en la formación tanto personal como profesional.

Han sido las **neurociencias** las que en las últimas décadas nos han permitido conocer tanto más del funcionamiento de nuestra propia mente que nunca antes. Los análisis con modernos equipos nos han permitido crear una especie de **cartografía cerebral** donde podemos ver reflejadas incluso las emociones, y nos han ayudado a comprender hasta qué punto somos seres sensibles al entorno. También se han aplicado los principios de las neurociencias a otras áreas como el marketing y la publicidad, y en la actualidad se está buscando desde esas herramientas **el santo grial de la educación**.

El ideal del siglo XXI, tanto en el trabajo como en la educación, se deberá basar en la **actividad colaborativa** y en equipo apoyada en las redes sociales, comunidades virtuales y **espacios de diálogo** que permitan la interrelación.

Frente a este panorama cuya **creciente complejidad** puede resultar avasallante, debemos educar a los niños para que puedan aprender a **tomar sus propias decisiones** en el camino, ya que ninguna será trivial, a la vez que les enseñemos que **el éxito nunca está garantizado** y que por eso deben transitar sendas que puedan disfrutar a cada instante, donde el punto de llegada y la meta sean un regalo adicional y **no el centro** de su vida. En un mundo de **exitismo acérrimo**, donde la desigualdad está a la orden del día, **saber vivir el presente** disfrutando del camino será el mejor legado que le podamos dejar a las futuras generaciones.

RESUMEN

En este capítulo final hemos englobado muchos de los temas tratados a lo largo del libro para poder concluir con el análisis de una temática tan compleja como es la de los menores en Internet y de la relación entre los niños y la tecnología. También hemos analizado algunos vínculos entre el futuro potencial y el presente, y el rol de la educación en el camino por recorrer. Por último, hemos dejado planteado un posible enfoque integral de la problemática y las situaciones asociadas, que seguramente debamos esperar algunos años para poder contrastar con los hechos.

Actividades

TEST DE AUTOEVALUACIÓN

1. Identifique grupos de interés o proyectos relacionados con el uso adecuado de las tecnologías e Internet y considere unirse a alguno para colaborar.
2. Evalúe la manera en que está utilizando las tecnologías de la información y, si es necesario, cambie los comportamientos que introducen riesgos evitables.
3. Busque en sitios de videos como YouTube, Vimeo, etcétera, algunos canales especializados en la concientización de menores en Internet para contar con material audiovisual de referencia.
4. Difunda los riesgos que introduce el uso de Internet entre las personas que considere que puedan necesitarlo y entre los futuros padres de familia.
5. La próxima vez que incorpore una nueva tecnología en el hogar que pueda ser utilizada por menores, asegúrese de haber analizado todos los riesgos asociados a su uso.

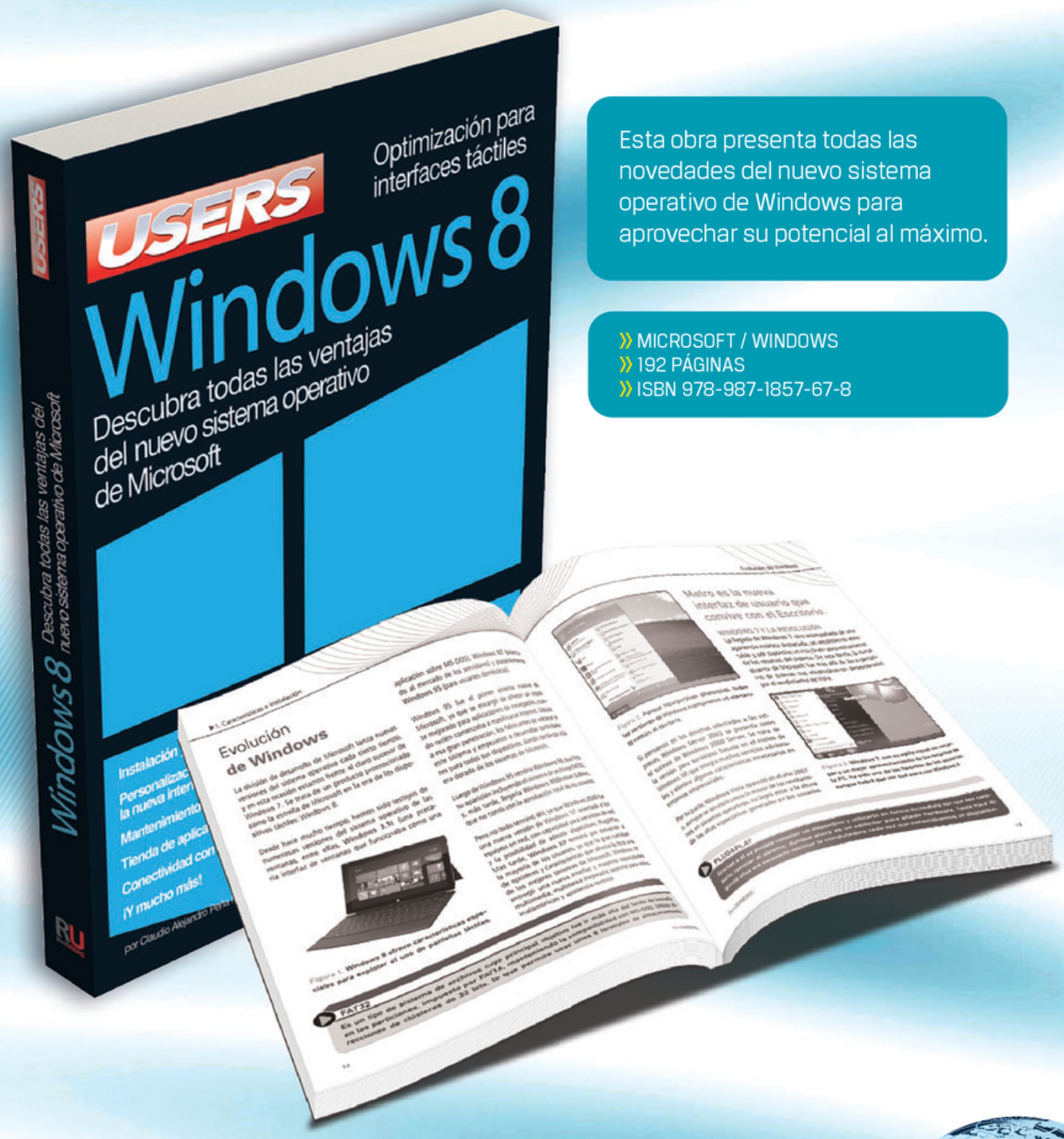


PROFESOR EN LÍNEA

Si tiene alguna consulta técnica relacionada con el contenido, puede contactarse con nuestros expertos:

profesor@redusers.com

CONÉCTESE CON LOS MEJORES LIBROS DE COMPUTACIÓN



Esta obra presenta todas las novedades del nuevo sistema operativo de Windows para aprovechar su potencial al máximo.

» MICROSOFT / WINDOWS
» 192 PÁGINAS
» ISBN 978-987-1857-67-8

LLEGAMOS A TODO EL MUNDO VÍA OCA* Y DHL**

MÁS INFORMACIÓN / CONTÁCTENOS

usershop.redusers.com +54 (011) 4110-8700 usershop@redusers.com

*SÓLO VÁLIDO EN LA REPÚBLICA ARGENTINA // **VÁLIDO EN TODO EL MUNDO EXCEPTO ARGENTINA

USERS

LOS MENORES Y LOS RIESGOS DE LAS NUEVAS TECNOLOGÍAS

Este libro presenta los conceptos más importantes relacionados con el impacto de las nuevas tecnologías en los menores, analizando el contexto de Internet, los videojuegos, los celulares y otros aspectos que ningún padre o educador puede dejar de tener en cuenta. Las experiencias presentadas se derivan de numerosas conferencias y conversaciones con niños de todas las edades, apoyadas por revisiones profesionales de psicólogos, pedagogos, educadores y otros expertos. Los resultados también se han enriquecido gracias a la gran cantidad de diálogos con padres y docentes inmersos directamente en la problemática. Este marco de referencia ayuda a comprender un mundo regido por la tecnología, en donde saber adaptarse a los cambios permite disfrutar de sus beneficios minimizando los riesgos.

> **Acompañar a los más chicos en el uso responsable de la tecnología es clave para protegerlos de los riesgos.**

EN ESTE LIBRO APRENDERÁ:

- **Introducción:** la era de la información. Internet y los medios de comunicación. Transición generacional y protagonismo de los nativos digitales.
- **El escenario virtual:** análisis de las distintas tecnologías que rigen el entretenimiento y las relaciones sociales. Cómo proteger la identidad virtual y digital.
- **Los peligros de Internet:** tipos de contenido y legalidad. El software malicioso y los engaños online. Crear conciencia para proteger a los niños del acoso virtual.
- **El hogar moderno:** la familia, la tecnología y el protagonismo de la PC. Usos de celulares, smartphones, notebooks y tablets. Qué límites podemos aplicar.
- **Desafíos del educador:** las tecnologías como parte activa del proceso educativo y el nuevo rol del docente. Consejos para mejorar el alcance de los objetivos.
- **Marco jurídico y visión de futuro:** legislación actual y nuevas necesidades. Análisis de la situación presente, abriendo el diálogo sobre un futuro posible.



SOBRE EL AUTOR

Federico Pacheco es especialista en seguridad de la información orientado a la consultoría, la investigación y la educación. Cuenta con más de 10 años de experiencia docente en distintos niveles de enseñanza y ha generado gran cantidad de material educativo para instituciones y para la comunidad en general.

NIVEL DE USUARIO

Básico / Intermedio

CATEGORÍA

Home - Internet - Seguridad





ISBN 978-987-1949-11-3

9 789871 949113 >

RU RedUSERS

REDUSERS.com
En nuestro sitio podrá encontrar noticias relacionadas y también participar de la comunidad de tecnología más importante de América Latina.

PROFESOR EN LÍNEA
Ante cualquier consulta técnica relacionada con el libro, puede contactarse con nuestros expertos: profesor@redusers.com.