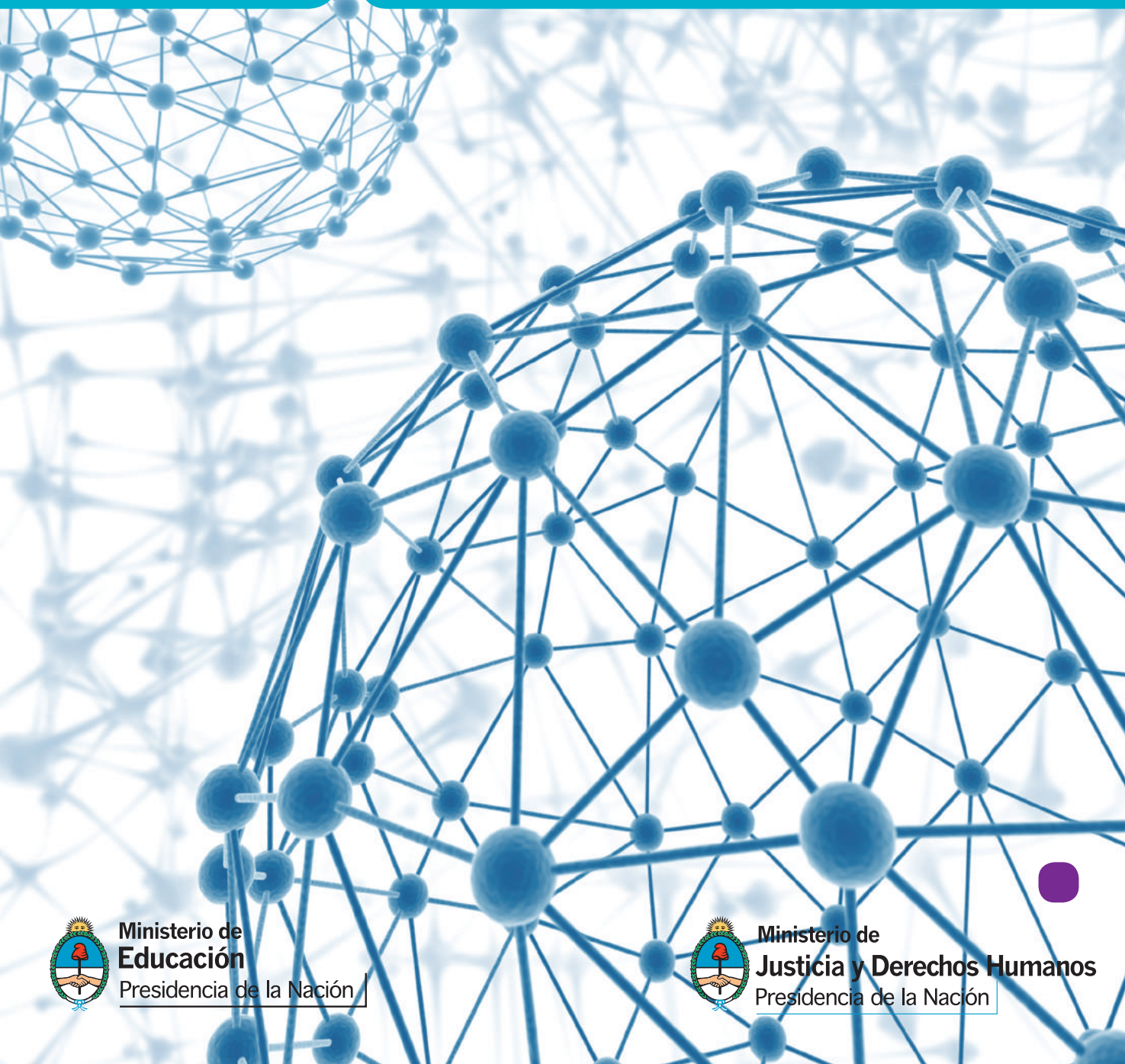
educ.ar

con vos en la web

Datos personales y nuevas tecnologías

Serie estrategias en el aula para el modelo 1 a 1



Ministerio de Educación
Presidencia de la Nación

Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

Presidenta de la Nación
Dra. Cristina Fernández de Kirchner

Jefe de Gabinete de Ministros
Dr. Juan Manuel Abal Medina

Autoridades del Ministerio de Educación

Ministro de Educación
Prof. Alberto E. Sileoni

Secretario de Educación
Lic. Jaime Perczyk

Jefe de Gabinete
A. S. Pablo Urquiza

Subsecretario de Equidad y Calidad Educativa
Lic. Gabriel Brener

Subsecretaria de Planeamiento Educativo
Prof. Marisa Díaz

Subsecretario de Coordinación Administrativa
Arq. Daniel Iglesias

Director Ejecutivo del INET
Lic. Eduardo Aragundi

Directora Ejecutiva del INFOD
Lic. Verónica Piovani

Directora Nacional de Gestión Educativa
Lic. Delia Méndez

Autoridades de Educ.ar

Gerente General
Lic. Rubén D'Audia

Gerente de TIC y Convergencia
Patricia Pomiés

Coordinación de Contenidos
Lic. Cecilia Sagol

Coordinación Editorial
Lic. Inés Roggi

Coordinación Multimedia
Lic. Alejandro Alejandro Vagnenkos

Coordinación de Proyectos
Lic. Mayra Botta

Coordinación de Tecnología
Lic. Juan Jolis

Autoridades del Ministerio de Justicia y Derechos Humanos

Ministro de Justicia y Derechos Humanos
Dr. Julio Alak

Secretario de Justicia
Dr. Julián Alvarez

Subsecretario de Coordinación y Control de Gestión Registral
Dr. Ernesto Kerplak

Director Nacional de Protección de Datos Personales
Prof. Dr. Juan Antonio Travieso

Coordinador Programa Con Vos en la Web
Ezequiel Passeron

con vos en la web

educar

Autores:
María Elena Qués.

Edición:
Juan Francisco Correas.

Corrección:
Verónica Andrea Ruscio.

Diseño de colección:
Silvana Caro.

Diagramación:
bonacorsi diseño.

Fotografía:
Stock.xchng (tapa), educ.ar.

Coordinador del Programa Conectar Igualdad:
Pablo Pais.

Directora del portal Educ.ar:
Patricia Pomiés.

Coordinador de Proyectos Educ.ar S. E.:
Mayra Botta.

Coordinación de Contenidos Educ.ar S. E.:
Cecilia Sagol.

Líder del proyecto Educ.ar S. E.:
Cristina Viturro.

www.educ.ar - Ministerio de Educación

Serie estrategias en el aula para el modelo 1 a 1

Datos personales y nuevas tecnologías

María Elena Qués

Prólogo

Hemos emprendido un camino ambicioso: sentar las bases para una escuela secundaria pública inclusiva y de calidad, una escuela que desafíe las diferencias, que profundice los vínculos y que nos permita alcanzar mayor igualdad social y educativa para nuestros jóvenes. En este contexto, el Programa Conectar Igualdad, creado por decreto del gobierno nacional N.º 459/10, surge como una política destinada a favorecer la inclusión social y educativa a partir de acciones que aseguren el acceso y promuevan el uso de las TIC en las escuelas secundarias, en las escuelas de educación especial y entre estudiantes y profesores de los últimos años de los Institutos Superiores de Formación Docente.

Tres millones de alumnos de los cuales somos responsables hoy integran el programa de inclusión digital. Un programa en el que el Estado asume el compromiso de poner al alcance de todos y todas la posibilidad de acceder a un uso efectivo de las nuevas tecnologías. Un programa que le otorga a la escuela el desafío de ofrecer herramientas cognitivas y el desarrollo de competencias para actuar de modo crítico, creativo, reflexivo y responsable frente a la información y sus usos para la construcción de conocimientos socialmente válidos.

En nuestro país, esta responsabilidad cobró vida dentro de la Ley de Educación Nacional N.º 26.206. En efecto, las veinticuatro jurisdicciones vienen desarrollando de manera conjunta la implementación del programa en el marco de las políticas del Ministerio de Educación de la Nación, superando las diferencias políticas con miras a lograr este objetivo estratégico.

Para que esta decisión tenga un impacto efectivo, resulta fundamental recuperar la centralidad de las prácticas de enseñanza, dotarlas de nuevos sentidos y ponerlas a favor de otros modos de trabajo con el conocimiento escolar. Para ello, la autoridad pedagógica de la escuela y sus docentes necesita ser fortalecida y repensada en el marco de la renovación del formato escolar de nuestras escuelas secundarias.

Sabemos que solo con equipamiento e infraestructura no alcanza para incorporar las TIC en el aula ni para generar aprendizajes más relevantes en los estudiantes. Por ello, los docentes son figuras clave en los procesos de incorporación del recurso tecnológico al trabajo pedagógico de la escuela. En consecuencia, la incorporación de las nuevas tecnologías, como parte de un proceso de innovación pedagógica, requiere, entre otras cuestiones, instancias de formación continua, acompañamiento y materiales de apoyo que permitan asistir y sostener el desafío que esta tarea representa.

Somos conscientes de que el universo de docentes es heterogéneo y lo celebramos pues ello indica la diversidad cultural de nuestro país. Por lo tanto, de los materiales que en esta oportunidad ponemos a disposición, cada uno podrá tomar lo que le resulte de utilidad de acuerdo con el punto de partida en el que se encuentra.

En tal sentido, las acciones de desarrollo profesional y acompañamiento se estructuran en distintas etapas y niveles de complejidad, para cubrir todo el abanico de posibilidades: desde saberes básicos e instancias de aproximación y práctica para el manejo de las TIC, pasando por la reflexión sobre sus usos, su aplicación e integración en el ámbito educativo, la exploración y profundización en el manejo de aplicaciones afines a las distintas disciplinas y su integración en el marco del modelo 1 a 1, hasta herramientas aplicadas a distintas áreas y proyectos, entre otros. Asimismo, los docentes pueden participar de diversos dispositivos de capacitación: virtual, presencial, aplicada y general y de materiales, contenidos e instancias de formación que acompañan sus actividades de cada día.

Los materiales que aquí se presentan complementan las alternativas de desarrollo profesional y forman parte de una serie destinada a brindar apoyo a los docentes en el uso de las computadoras portátiles en las aulas, en el marco del Programa Conectar Igualdad. Esta es la segunda serie que les presentamos a los docentes, los directivos, los bibliotecarios, las familias y toda la comunidad educativa. En esta segunda etapa se privilegió la articulación directa de contenidos pedagógicos y tecnológicos y las prácticas del aula o la escuela; en todos los materiales se intenta brindar al docente sugerencias didácticas muy concretas para el uso de las TIC y a la vez información general para enmarcar el proceso del que están siendo protagonistas en la sociedad del conocimiento.

De esta manera, el Estado Nacional acompaña la progresiva apropiación de las TIC para mejorar prácticas habituales y explorar otras nuevas, con el fin de optimizar la calidad educativa y formar a los estudiantes para el desafío del mundo que los espera como adultos.

Deseamos que este importante avance en la historia de la educación argentina sea una celebración compartida, como parte de una política nacional y federal que tiene como uno de sus ejes fundamentales a la educación con inclusión y justicia social.

Prof. Alberto Sileoni
Ministro de Educación de la Nación

Índice

1 Introducción

El acceso masivo de los estudiantes a las nuevas tecnologías de la información y la comunicación (TIC), y con ellas a internet, no consiste solamente en el uso de computadoras: se trata de nuevas formas de conocer, de acceder a múltiples saberes y también de un nuevo mundo de prácticas culturales y de relaciones sociales cotidianas.

Contactos sociales en redes —según intereses, relaciones previas o, simplemente porque sí—, intercambios de información, compras y ventas, trabajos, etc. Estas son prácticas que generan nuevas formas de consumo y sociabilidad en la vida de todos los días.

Si bien esta transformación atraviesa todas las generaciones, los jóvenes se han apropiado de las TIC de una manera especial, tanto por frecuencia como por forma de uso.

En América Latina, Chile (82 %) y la Argentina (79 %) son los países en los que hay más cantidad de hogares con computadoras entre los mayores de diez años. La Argentina tiene, a su vez, la mayor penetración de internet entre los adolescentes (57 %), junto con Brasil.[1] Asimismo, un trabajo del Ministerio de Educación de la Nación señala que siete de cada diez chicos de 11 a 17 años en la Argentina tienen computadora en su casa y forman parte de una red social; poseen teléfono móvil y lo usan principalmente para enviar y recibir mensajes, en segundo lugar para escuchar música y, en tercer lugar, para comunicarse con sus padres.[2]

Con respecto a los cambios en el modo de consumo, señala Sergio Balardini:

"La primera cuestión que hay que tener en cuenta es que ya no hay un adentro y un afuera de la tecnología. Los chicos usan internet como un continuo de sus vidas reales. Por esta vía, siguen haciendo cosas que ya venían haciendo, como por ejemplo, escuchar música. Además, ven videos y buscan mucha información. Los chicos se informan, prácticamente, a través de internet y la televisión. Otra cosa, por supuesto, es permanecer conectados por medio del chat. Está naturalizado que los jóvenes que tienen las condiciones materiales para hacerlo —es decir, que cuentan con computadora en sus casas— llegan y encienden la computadora, y dejan el chat permanentemente abierto. Las nuevas tecnologías facilitan estar conectados permanentemente."[3]

Henry Jenkins, profesor e investigador del MIT Comparative Media Studies Program, señala que los jóvenes son parte de lo que denomina "cultura colaborativa", [4] la cual incluye prácticas organizadas a través de consumos multimedia, la existencia de comunidades y la participación en espacios de creatividad.

* notas

1. Fundación Telefónica: *La generación interactiva en la Argentina*. Recuperado de http://www.telefonica.com.ar/corporativo/acercadetelefonica/ar/usoresponsable/PDFs/GeneracionInteractivaArgentina.pdf [consultado el 21/03/2013].
2. Ministerio de Educación: *Consumos digitales culturales*. Recuperado de http://bibliotecadigital.educ.ar/uploads/contents/TIC_ConsumosCulturalesPARAokFINAL1.pdf [consultado el 21/03/2013].
3. Balardini, Sergio: «¿Estás seguro?», en *Conectados La Revista*, (n.° 1). Recuperado de http://bibliotecadigital.educ.ar/articles/read/283 [consultado el 21/03/2013].
4. Jenkins, Henry: *Building the field of Digital Media and Learning*, Chicago, MacArthur Fundation, 2009.

Para relacionarse en estos ambientes, los jóvenes desarrollan altas capacidades de manejo de software y plataformas, como así también competencias de negociación, resolución de problemas, lenguajes transmedia, etcétera.

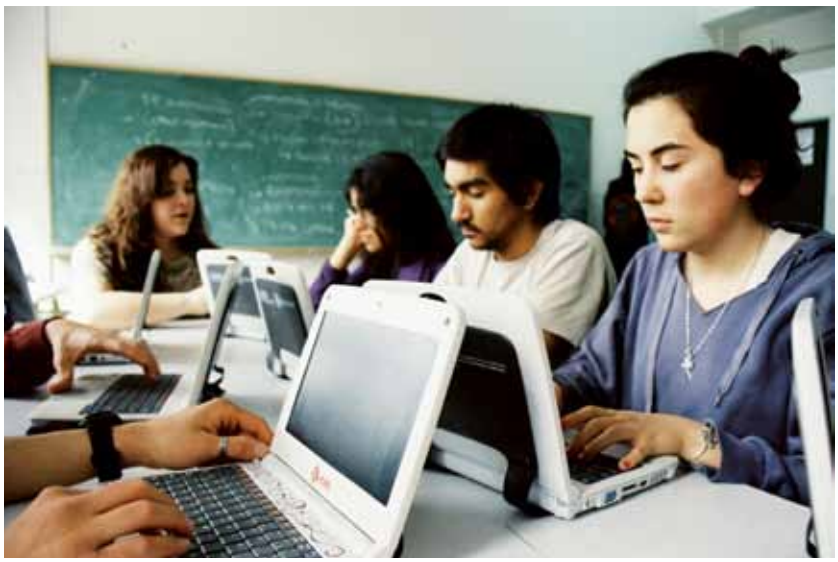
Si bien la adquisición de estas capacidades se realiza, en gran medida, mediante aprendizajes informales, Jenkins señala que, no obstante, hay espacios que requieren necesariamente la intervención de la escuela, del docente o de los padres.

Esto significa algo que contradice la opinión común: los chicos no dominan completamente el mundo digital. Hay determinados aspectos que los jóvenes no saben y no pueden aprender solos. Entre estos aspectos se encuentra el área del comportamiento ético y los cuidados en internet.

La incorporación de las TIC genera a las escuelas y a las familias un nuevo desafío: acompañar a los jóvenes en el uso de los espacios sociales que promueve internet, ayudarlos, protegerlos y enseñarles a aprovecharlos con responsabilidad, para no ser dañados y no dañar.

De esta manera, cualquier propuesta educativa, que involucre educación con TIC —que es la tendencia en la escuela de hoy— y que busque dialogar con las prácticas culturales de los adolescentes en la era de las culturas participativas tiene que incluir el tema de los comportamientos en internet.

Contactos con desconocidos, ciberacoso (*cyberbullying*), respeto por la privacidad propia y ajena, compras y ventas en línea, descargas peligrosas para la computadora son algunas de las problemáticas que se abren cuando el mundo virtual se transforma en un lugar de prácticas sociales.

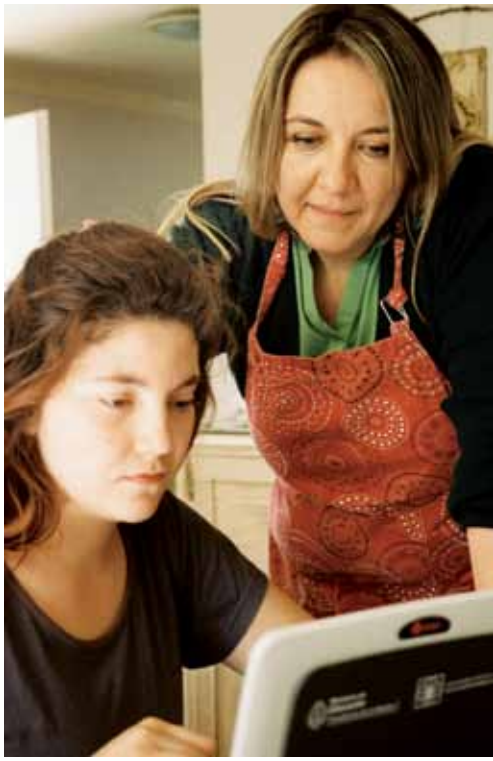


Muchas de estas cuestiones se relacionan con formas de comportamiento, normas y límites tradicionales en otros entornos; otras, con nuevas prácticas y situaciones propias del medio digital. En este último grupo, se encuentra la protección de datos personales, un tema que es necesario que los jóvenes aprendan a manejar, por su envergadura como problemática en el mundo digital, por su relación con el mundo del derecho y porque atraviesa varios de los puntos críticos de la relación de los chicos con las nuevas tecnologías.

Este material, destinado a docentes y directivos, que también puede ser aprovechado por las familias, tiene el objetivo de informar sobre problemas y riesgos, brindar consejos para su prevención y fomentar buenas prácticas en la red. También se sugieren actividades para realizar en el aula y en la escuela, para que los estudiantes reflexionen sobre estos temas, conozcan la información, comprendan las normas de comportamiento y puedan aprovechar la riqueza de internet de manera responsable.

Es importante que docentes, directivos y padres estén informados sobre estos temas, ya que es conocimiento que se debe transmitir a los niños y jóvenes como parte de su educación.

La información brindada es la más actualizada al momento de publicación. Sin embargo, hay que tener en cuenta que internet es un medio muy dinámico y algunas referencias —por ejemplo, a los protocolos de compra segura o a los programas antivirus— pueden cambiar en poco tiempo. Se requiere una actitud activa e informada en forma permanente.



Este cuadernillo apunta a brindar a los docentes:

- información, definiciones, conceptos, introducción a la problemática relacionada con la seguridad en internet;
- consejos e instrucciones para desarrollar buenas prácticas en las interacciones desarrolladas en internet;
- sugerencias de actividades, proyectos con TIC para trabajar en el aula, la escuela y el hogar.

La protección de datos como un derecho

Desde la perspectiva del derecho, la protección de datos personales está basada en el derecho a la privacidad, que es uno de los derechos humanos consagrado y garantizado en la Constitución Nacional. Nadie puede ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o

Ver página 14 para una definición completa de datos personales.

su correspondencia, ni de ataques a su honra o a su reputación, y la ley debe proteger a las personas contra tales injerencias o ataques. En la Argentina, este derecho está amparado por la Ley 25.326, sancionada en 2001.[5]

Por otra parte, todas las personas tenemos el derecho de conocer quién tiene nuestros datos, para qué los tiene y cuál es su fin último, es decir, tener control sobre ellos, para proteger nuestro honor, intimidad y privacidad. La protección de datos que garantiza la ley incluye a los que circulan en internet a través de computadoras, teléfonos celulares y otros dispositivos.

A continuación, se enuncian algunos de los derechos promulgados por esta ley.

Derecho de información. Toda persona puede saber, por ejemplo, qué datos sobre ella tiene una empresa. Para ello se puede consultar a la Dirección Nacional de Protección de Datos Personales, un órgano nacional de control de datos, perteneciente al Ministerio de Justicia y Derechos Humanos de la Nación Argentina.

En la DNPDP, se brinda toda la información de contacto de esa empresa, entre otros servicios. Consultas en http://www.jus.gob.ar/datos-personales.aspx.

Derecho de acceso. Con solo demostrar su identidad, toda persona tiene derecho a conocer la información personal que está disponible en una base de datos pública o privada.

Derecho de actualización. Si los datos personales figuran en una base de datos de manera incorrecta, las personas tienen derecho a pedir que sean corregidos o actualizados de manera gratuita, o que no se den a conocer a otras personas.

Derecho de rectificación, actualización o supresión. Es posible pedir que se elimine, en forma gratuita, información falsa o disponible sin autorización o por error.

En la Dirección Nacional de Protección de Datos Personales, toda persona puede obtener asesoramiento gratuito por vía telefónica o en persona. http://www.jus.gob.ar/datos-personales.aspx

Mesa de entradas: (011) 5300-4000, internos 76705/76730/76721
Registro de bases de datos: (011) 5300-4000, internos 76725/76727/76737/76736
Denuncias: (011) 5300-4000, internos 76723/76724/76742
Consentimientos informados: (011) 5300-4000, internos 76704/76732
Inspecciones: (011) 5300-4000, internos 76714/76729
Registro Nacional de Documentos de Identidad Cuestionados: (011) 5300-4000, interno 76707
Con vos en la web: (011) 5300-4000, interno 76712/76709

* notas

5. Honorable Cámara de Diputados de la Nación: Ley 25.326. *Protección de datos personales*. Recuperado de http://www1.hcdn.gov.ar/dependencias/dip/textos%20actualizados/25326.010408.pdf [consultado el 21/03/2013].

Los e-derechos proclamados por Unicef

Para proteger a los niños y jóvenes, Unicef proclamó una declaración de derechos en internet.

1. Derecho al acceso a la información y la tecnología, sin discriminación por motivo de sexo, edad, recursos económicos, nacionalidad, etnia, lugar de residencia, etcétera. En especial este derecho al acceso se aplicará a los niños y las niñas discapacitados.
2. Derecho al esparcimiento, al ocio, a la diversión y al juego, también mediante internet y otras nuevas tecnologías. Derecho a que los juegos y las propuestas de ocio en internet no contengan violencia gratuita, ni mensajes racistas, sexistas o denigrantes y respeten los derechos y la imagen de los niños y las niñas, de otras personas.
3. Derecho a la intimidad de las comunicaciones por medios electrónicos. Derecho a no proporcionar datos personales por la red, a preservar su identidad y su imagen de posibles usos ilícitos.
4. Derecho al desarrollo personal y a la educación, y a todas las oportunidades que las nuevas tecnologías como internet puedan aportar para mejorar su formación. Los contenidos educativos dirigidos a niños y niñas deben ser adecuados para ellos y promover su bienestar, desarrollar sus capacidades, inculcar el respeto a los derechos humanos y al medio ambiente y prepararlos para ser ciudadanos responsables en una sociedad libre.
5. Derecho a beneficiarse y a utilizar en su favor las nuevas tecnologías para avanzar hacia un mundo más saludable, más pacífico, más solidario, más justo y más respetuoso con el medio ambiente, en el que se respeten los derechos de todos los niños y niñas.
6. Derecho a la libre expresión y asociación, a buscar, recibir y difundir información e ideas de todo tipo por medio de la red. Estos derechos solo podrán ser restringidos para garantizar la protección de los niños y niñas de información y materiales perjudiciales para su bienestar, desarrollo e integridad; y para garantizar el cumplimiento de las leyes, la seguridad, los derechos y la reputación de otras personas.
7. Derecho de los niños y niñas a ser consultados y a dar su opinión cuando se apliquen leyes o normas a internet que afecten, como restricciones de contenidos, lucha contra los abusos, limitaciones de acceso, etcétera.
8. Derecho a la protección contra la explotación, el comercio ilegal, los abusos y la violencia de todo tipo que se produzcan utilizando internet. Los niños y niñas tendrán el derecho de utilizar internet para protegerse de esos abusos, para dar a conocer y defender sus derechos.

9. Los padres tendrán el derecho y la responsabilidad de orientar, educar y acordar con sus hijos un uso responsable de internet: establecer tiempos de utilización, páginas que no se deben visitar o información que no deben proporcionar para protegerles de mensajes y situaciones peligrosas, etcétera. Para ello, las familias también deben poder formarse en el uso de internet e informarse sobre sus contenidos.
10. Los gobiernos de los países desarrollados deben comprometerse a cooperar con otros países para facilitar el acceso de estos y sus ciudadanos, y en especial de los niños y niñas, a internet y otras tecnologías de la información para promover su desarrollo y evitar la creación de una nueva barrera entre los países ricos y los pobres.

Los jóvenes y la protección de los datos

Por lo general, los jóvenes no tienen información sobre los diversos peligros y la necesidad de proteger los datos personales, por lo que se manejan con relativa ingenuidad en el uso de las redes sociales y el consumo de datos en la web. Pero la necesidad de proteger los datos aparece en un contexto marcado por las siguientes variables:

- La conexión permanente y ubicua —en todo lugar— a través de las tecnologías móviles incrementó el tiempo de contacto entre los jóvenes y el mundo virtual y la posibilidad de contactarse con personas y contenidos en tiempo real. En este marco, según muestran algunos estudios sobre los consumos de los jóvenes en internet,[6] los jóvenes tienden a borrar las divisiones entre el mundo sin conexión y el mundo en línea; a ignorar la diferencia entre actuar en el mundo presencial y hacerlo en internet, donde algo dicho o publicado permanece, se hace público y se multiplica.
- La cultura participativa —tal como la definió Jenkins— está basada en el uso de ambientes colaborativos, es decir, redes sociales, redes de juegos, sitios para comprar y descargar herramientas y programas, videos, etcétera. Durante esta participación, los jóvenes suelen publicar en el espacio público información personal.
- Más allá de la cultura juvenil, la sociedad de la información conduce a que cada vez, en mayor medida, todas las generaciones realicen actividades en forma digital. De esta manera, la adquisición de competencias para el cuidado de los datos personales es valiosa tanto para los jóvenes como para los adultos para manejarse en estos espacios cada vez más habituales.
- Finalmente, el uso de TIC en la escuela también promueve la utilización de plataformas colaborativas, redes sociales, aulas virtuales, bibliotecas, portales, etcétera, en el aprendizaje. En este sentido, los jóvenes también brindan datos personales cuando realizan su trabajo escolar buscando información, diseñando blogs y participando en internet de diversas maneras.

* notas

6. Ministerio de Educación: *Chic@s y Tecnología. Usos y costumbres de niñas, niños y adolescentes en relación a las* TIC. Recuperado de http://coleccion.educ.ar/coleccion/CD27/datos/investigacion-chicos-net-chicos-tecnologia.html [consultado 21/03/2013].

2 La información personal

Los datos personales son información de cualquier tipo que pueda ser usada para identificar, contactar o bien localizar a una persona. Entre ellos se encuentran: nombre y apellido, número de documento, nacionalidad, sexo, estado civil, número de teléfono, número de celular, huellas digitales, dirección de correo electrónico, número de tarjeta de crédito o débito, número de cuenta bancaria, fotos, videos, publicaciones, ubicación espacial, actividades, opiniones, etcétera.

Dentro de los datos personales existe un grupo de ellos, denominados *datos sensibles*, que exige mayor protección. Estos se refieren a ciertas circunstancias que hacen a la vida íntima de un sujeto y deben ser tratados de manera diferente, ya que requieren un mayor cuidado. Estos datos son los que revelan: origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

Los datos personales en internet

Hay tres tipos diferentes de datos personales que se dejan en la web al navegar. Estos son:

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

Los datos aportados voluntariamente

Se facilitan datos personales en variadas ocasiones:

- En el momento de solicitar el alta como usuario de un sitio web, correo electrónico o red social, se suele pedir nombre y apellido, correo electrónico, fecha de nacimiento, entre otros datos.
- Al realizar la compra de un objeto o pagar un servicio a través de internet, además de los datos antes mencionados, se deja el número de una tarjeta de crédito.
- Durante el uso de redes sociales, foros, etcétera, se aportan datos sobre los gustos, las preferencias personales, o la ubicación.

El portal educ.ar, por ejemplo, informa a sus usuarios de la privacidad de los datos que brinden en la web cuando se registran en http://portal.educ.gov.ar/acercade/condiciones.php. En este apartado, el portal explica qué datos de los usuarios solicita y para qué los usa, y aclara, por ejemplo:

Nosotros no utilizamos ni revelaremos a terceros información individual respecto de sus visitas a Educ.ar o información que pueda proporcionarnos, tal como su nombre, dirección, dirección de correo electrónico o número telefónico. No obstante, y como se mencionó anteriormente, es práctica de la empresa compartir con empresas vinculadas al Portal y las entidades dependientes y/o bajo el control del Ministerio de Educación de la Nación, la información estadística acerca del uso del Portal.

Educ.ar invierte sus mejores esfuerzos para proteger la identidad y los datos personales de sus usuarios. Educ.ar no venderá, alquilará ni negociará con otras empresas u organizaciones su información personal. Toda la información personal que usted transmite se hace a través de una página de internet segura que protege su información.

Al volcar información de la tarjeta de crédito —existe la posibilidad de que los jóvenes tengan la suya propia o pidan prestada la de algún adulto—, se debe comprobar que la compra sea segura.[7] Existen sellos internacionales que garantizan que un sitio de compras manejará los datos con seguridad. Por ejemplo, el método SSL (*Secure Sockets Layer* o capa de conexión segura, en español), implica que los servidores del sitio son seguros, que los datos están encriptados, que se guardan fuera de línea y que serán destruidos después de la transacción. Para indicar que la información será encriptada, se incluyen un URL que comienza con "https:" en lugar de "http:" y el ícono de un candado en la parte inferior derecha de la ventana.

Cuando se solicitan datos personales, por ejemplo, para una encuesta o un concurso, es importante saber que, de acuerdo con el Art. 4 de la Ley de Protección de Datos Personales —que aborda el tema de la calidad de los datos—, las preguntas para obtener información deben ser: adecuadas, pertinentes y no excesivas en relación con el ámbito y la finalidad para la cual se obtienen. Es decir, hay que tomar conciencia de la finalidad para la cual se pide la información y analizar si el pedido es pertinente. Si no parece adecuado, hay que omitir la cesión de esos datos.

+ Información

El proceso de encriptación toma la información ingresada y la convierte en códigos de bits que son transmitidos mediante protocolos de seguridad a través de internet. Estos datos desarmados no pueden ser leídos mientras la información viaja a través de la web. Una vez que la información personal encriptada es recibida por los servidores seguros, harían falta miles de años de la computadora más potente del mundo para decodificar el mensaje, lo que garantiza que si alguien intercepta la comunicación no podrá interpretarla.

Actividades

- Investigar, en forma colaborativa, qué declaraciones de privacidad tienen los sitios y las plataformas que los alumnos visitan habitualmente.
- Ir a este enlace y realizar la actividad 1. http://www.convosenlaweb.gob.ar/media/413326/cvelw_actividad_adolescentes.pdf

* notas

7. El video *Comprando en internet*, de la Jefatura de Gabinete de Ministros de Presidencia de la Nación aporta información sobre este tema. Recuperado de http://www.youtube.com/watch?v=3P6Kzwo5eZg [consultado el 21/03/2013].

Los datos publicados por terceros

Muchas veces se pueden encontrar en internet datos personales que las personas no han publicado ni han consentido expresamente. Puede ocurrir en sitios web, redes sociales, portales de video, blogs, foros, boletines, etcétera. Esto ocurre cuando:

- una persona etiqueta a otra en una red social o sube una foto, sin consentimiento, en la que aparecen varias personas;
- alguien publica en un sitio o blog información de otras personas;
- el Estado difunde información pública sobre los ciudadanos.

En la web, los datos personales se replican, son enlazados por otros sitios, comienzan a aparecer en los buscadores y alcanzan una difusión global.

Es importante saber que las personas tenemos derecho a que se supriman los datos publicados en sitios web que no cuentan con nuestro consentimiento.
En Facebook, por ejemplo, hay una opción para configurar la privacidad de las etiquetas: https://www.facebook.com/settings/?tab=privacy.
Del mismo modo, los usuarios deben ser responsables cuando publican imágenes, información o referencias de terceros. Es importante que los jóvenes adquieran la costumbre de pedir permiso a sus amigos cuando los van a mencionar, incluir, fotografiar, etiquetar o citar en redes sociales y que sepan que pueden pedir a la persona que haya posteado algo sin su consentimiento que retire la publicación.

Actividades

- Conectados a internet, buscar información sobre algunos de los alumnos o el docente, poniendo el nombre en buscadores y redes sociales. Luego, analizar los resultados:
  ¿Qué datos tiene la web sobre cada uno?
  ¿Qué datos fueron ingresados por la misma persona?
  ¿Qué datos de los que están en la web pueden considerarse "datos sensibles"?
- Realizar un debate presencial o un foro virtual a partir de las siguientes preguntas:
  Si subimos la imagen de otra persona a una red social, ¿debemos avisarle o pedirle autorización? ¿En todos los casos o solo si es una foto comprometedora?
- Ir al siguiente enlace, leer y resumir la información. Verificar si es útil, correcta y suficiente.
  http://www.masfb.com/2011/10/configuracion-etiquetas-facebook.html#.UQqOFx1awll

3 La protección de los datos en internet

Al navegar por la web se brinda información de manera involuntaria. Esto sucede porque la computadora envía señales que son interpretadas por servidores que la procesan como datos. Cada computadora tiene un número —llamado *dirección IP*—, que la identifica dentro de la red. Esta etiqueta numérica es registrada por los sitios que se visitan.

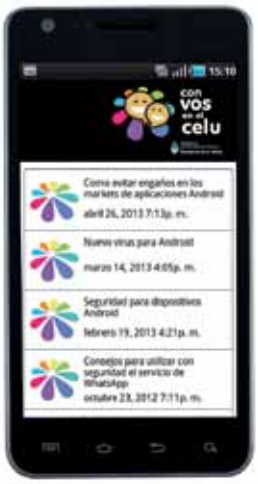
Al mismo tiempo, algunos sitios —por ejemplo, de publicidad— envían archivos que se almacenan en la computadora. Se denominan *cookies* y envían información a estos sitios sobre las actividades que se realizan en esa máquina. De esta manera, hay sitios web que pueden detectar fácilmente cómo se navega por internet, ver los gustos y preferencias de cada usuario, hacer estrategias de *marketing* y elaborar perfiles de comportamiento.

Para evitar que quede registro de los recorridos realizados en internet, se recomienda realizar en la computadora algunos procedimientos:

- borrar regularmente las cookies que almacena la PC. Están en una carpeta con ese nombre, en el disco C. En el sistema operativo de la computadora o del navegador, se indica cómo hacerlo.
- borrar regularmente el historial de navegación. Muchos navegadores tienen una herramienta que se denomina *Do not track* (no rastrear), que reduce las huellas que se dejan durante la navegación. Más información sobre el tema en este enlace: http://prezi.com/ctkk48uwwyo-/cookies-y-do-not-track/?kw=view-ctkk48uwwyo-&rc=ref-13473394 [consultado el 22/03/2013].

Algunos navegadores tienen la opción "Navegación en modo incógnito" —también llamado *protegido* o *privado*— que puede ser configurada por el usuario y que hace que las páginas a las que el usuario accede no aparezcan en los historiales de búsqueda del navegador, y no deja ningún rastro en la computadora. Esta función se encuentra entre las opciones de los navegadores en el menú "Herramientas" o "Configuración".

Los datos personales en los dispositivos móviles



Los teléfonos inteligentes o *smartphones* son dispositivos móviles que permiten al usuario tener en su propio teléfono celular funciones que antes eran reservadas para las computadoras.

Gracias a las plataformas informáticas móviles, estos celulares permiten acceder a internet, consultar la cuenta de correo electrónico, acceder a redes sociales, juegos en línea, etcétera.

La posibilidad de tener en un mismo dispositivo funciones que antes se daban en varios —teléfono, computadora, reproductor musical— se denomina *convergencia*. Es una consecuencia del mundo digital y genera enormes posibilidades para los usuarios. Sin embargo, estos dispositivos requieren cuidados especiales.

En la Argentina, en el año 2009, la Universidad de Palermo y TNS Gallup[8] encuestaron a jóvenes de todo el país, de entre 10 y 24 años, sobre el uso de tecnología. El 40 % de los entrevistados —más allá de las diferencias económicas— señaló el celular como el dispositivo preferido, muy por encima de la computadora (23 %) y del televisor (34 %).

Portátil y fácil de perder

Es más fácil perder o que roben un celular que una computadora. La portabilidad de dispositivos con muchos datos puede hacer que gran cantidad de información personal quede en otras manos. Los teléfonos de contactos, el acceso a las cuentas de correo electrónico y redes sociales, imágenes y videos personales, aplicaciones, etcétera, corren peligro si se pierde o es robado un dispositivo portátil de estas características.

Es importante tener el teléfono bloqueado con una contraseña, para que solo su propietario pueda usarlo y acceder al contenido. Esta clave debe actualizarse periódicamente y no debe ser compartida con nadie.

* notas

8. Universidad de Palermo y TNS Gallup: *La tecnología y los jóvenes argentinos*. Disponible en: http://www.palermo.edu/economicas/PDF_2009/UPGALLUP/UP-TNSUP3%20.pdf [consultado el 22/03/2013].

Aplicaciones, instalación y virus en teléfonos móviles

En los celulares y en las tabletas se pueden descargar aplicaciones, también llamadas *apps*. Las aplicaciones son programas para participar de juegos, obtener localizaciones, acceder a noticias, videos, música, etcétera desde el dispositivo móvil. En muchos casos son gratuitas y fáciles de descargar. Sin embargo, no todas son compatibles con todos los sistemas operativos. Hay que buscar y descargar solo las que puedan utilizarse.

Algunas aplicaciones que se ofrecen en forma gratuita resultan básicas y no sirven demasiado. Entonces, se invita al usuario a descargar una versión paga. En ese caso, se recomienda tomar las mismas precauciones que en otras compras en internet.

Algunas veces, al instalar una aplicación, se avisa al usuario que se utilizará información de su teléfono. Para evitar inconvenientes, se deben tomar los siguientes recaudos:

- No siempre es fácil saber a qué datos del teléfono podrá acceder la aplicación. Es necesario evaluar si esta es realmente útil y si la empresa que la desarrolla es confiable.
- Si el teléfono tiene sistema operativo Android, se puede leer la autorización antes de instalar las aplicaciones que toman datos. Hay que evaluar si los datos que la aplicación va a tomar son significativos para esa aplicación. Por ejemplo, una aplicación para informar el estado del tiempo no tiene por qué acceder a mensajes de texto, pero es lógico que acceda a la localización para informar el clima del lugar en donde se encuentra el usuario. Algunas aplicaciones permiten el acceso a datos que no están relacionados con el propósito de la aplicación. En este caso, no es recomendable instalarla.
- Un teléfono celular con acceso a internet puede infectarse con virus o programas maliciosos. Cuando esto sucede, el teléfono envía correos electrónicos o mensajes de texto que no han sido escritos por el usuario, o se instalan aplicaciones que el usuario no descargó. Para resolver el inconveniente, hay que asesorarse con el proveedor de telefonía celular o con la empresa que fabricó la aplicación. Existen empresas que proveen aplicaciones para proteger los datos de los teléfonos celulares, pero son relativamente nuevas.

Geolocalización a través del móvil

Para trabajar en clase con este concepto, se recomienda leer "Introducción al concepto de geolocalización e instalación del software Google Earth", recuperado de http://escritoriodocentes.educ.ar/datos/Introduccion_geolocalizacion_google_earth.html [consultado el 25/03/2013].

Se denomina *geolocalización* a la posibilidad de ubicar un dispositivo a través de sistemas de información geográfica (SIG). Los SIG son un conjunto de programas e instrumentos tecnológicos —software y hardware— que interpretan información geográficamente referenciada.

Los teléfonos móviles —así como las netbooks y las tabletas— pueden activarse para enviar información sobre el lugar en el que se encuentran porque cuentan con funciones especializadas, como los receptores de GPS (*Global Positioning Systems* o sistema de posicionamiento global) que, gracias a la red de satélites, permite determinar la posición de un objeto en cualquier parte del mundo.

Estos servicios de geolocalización pueden tener un gran impacto en la privacidad de los usuarios, ya que permiten el monitoreo constante de los datos de localización. Al conocer los hábitos y patrones de movimiento habituales, los proveedores pueden crear perfiles precisos de sus usuarios. El mayor riesgo reviste en que la mayoría de las personas no son conscientes de tener activados los dispositivos de localización de sus teléfonos móviles o tabletas —ya que muchas veces vienen activados "por defecto"— y, por ende, transmiten permanentemente su ubicación.

Todos los dispositivos tienen la posibilidad de desactivar la geolocalización. Se recomienda cancelarla y volver a activarla cuando sea necesario.

Actividades

La posibilidad de rastrear la ubicación de celulares en un mapa ha sido utilizada para desarrollar obras de arte de vanguardia. En este blog se puede observar cómo se realizó en los Estados Unidos un tributo a Steve Jobs a partir de esta tecnología: http://appleweblog.com/2011/08/arte-con-geolocalizacion-un-tributo-a-steve-jobs.

- Realizar una investigación y una muestra virtual de experiencias que reflejen de una manera artística la realidad de la localización.

Contraseñas seguras para el acceso a redes y sitios

La necesidad de contar con contraseñas sólidas y eficientes es uno de los aspectos más sencillos y útiles para trabajar con los alumnos la seguridad informática, ya que todos los sistemas pueden estar protegidos por una contraseña de acceso. En relación con este tema, los aspectos por considerar son los siguientes:

No usar la misma clave para todo. Lo más seguro es tener una contraseña distinta para acceder a cada uso: correo electrónico, red social, cajero automático, banco, etcétera, en el caso de los adultos. Los delincuentes cibernéticos suelen robar contraseñas de sitios web que cuentan con poca seguridad, y luego intentan replicar las mismas claves en entornos más seguros, como las webs de los bancos.

Claves largas, complejas, y si no tienen sentido, mejor. Las mejores contraseñas —es decir, las más difíciles de adivinar— son las largas, que contienen letras, números, signos de puntuación y símbolos. Hay palabras o frases inventadas por el usuario que pueden ser fáciles de recordar para él mismo e imposibles de descifrar para quien lo intente. Ejemplo: "Tengo1clave+segura".

No compartir las claves con nadie. Entre los niños a veces existe la costumbre de confiarse la contraseña como muestra de confianza. Es importante que los alumnos tengan en cuenta que las claves son personales y no deben ser compartidas con nadie. El usuario es el dueño de la cuenta y el dueño de la clave. Una contraseña no debe ser conocida más que por su dueño.

Contraseñas fáciles, pero difíciles de olvidar y de adivinar. Un truco es usar una palabra o frase fácil, pero cambiando las vocales por números. Por ejemplo: "Tengoalgoparadecirte" sería "T3ng0alg0parad3c1rt3" o utilizar símbolos. Por ejemplo: "vaca123", fácil de adivinar, quedaría convertida en "vaca!"#".

Usar mayúsculas. Utilizando la opción de las mayúsculas se agrega una dificultad más a quien quiera adivinar una clave. Esta puede ir al inicio o en cualquier parte de la contraseña. Ejemplo: "Equipo2013" o "eQuIPo2013".

Evitar información personal. No incluir en la contraseña el nombre, el apellido, la fecha de nacimiento, el número de documento o información de este tipo, ya que las que contienen este tipo de datos son las más fáciles de adivinar.

Cambiar la clave luego de un período de tiempo prudencial. Al usar equipos compartidos o redes públicas o al entrar en internet en sitios públicos, será prudente cambiar las claves de acceso utilizadas en dichos equipos y redes luego de determinado tiempo.

Preguntas secretas. Para registrarse en un sitio web, uno de los requisitos que surgen al completar los datos es establecer una pregunta secreta, por si alguna vez no se recuerda la clave o contraseña de acceso. En estos casos se deben elegir preguntas difíciles de adivinar y que eviten las respuestas obvias o de posibilidades reducidas. Ejemplo: "¿Cuál es mi color favorito?".

Guardar las claves en un documento de texto. Al elegir contraseñas largas, difíciles de memorizar, y variadas para los diferentes usos, puede ser útil almacenarlas en un archivo de texto dentro de la computadora.

Las contraseñas deben ser secretas, privadas, difíciles de averiguar y fáciles de recordar.

Actividades

- Pedir a los alumnos que realicen una encuesta para verificar el cuidado de sus compañeros en la selección de contraseñas. Para ello, deberán seguir los siguientes pasos:
  a. Redactar las preguntas, considerando los puntos vistos anteriormente.
  b. Realizar una muestra.
  c. Evaluar los resultados y sacar conclusiones sobre el tema.

  Para más información sobre cómo trabajar con encuestas en clase, consultar "¡Encuesta en la escuela!", recuperado de http://www.educ.ar/recursos/ver?rec_id=70793 [consultado el 25/03/2013].

Las redes wifi

Para trabajar el concepto de **ancho de banda** es interesante recurrir a Wikipedia. Recuperado de http://es.wikipedia.org/wiki/Ancho_de_banda [consultado el 25/03/2013].

Se denomina *wifi* a uno de los sistemas de redes de conectividad inalámbricas más utilizados. Se trata de conexión a internet sin cables, a través de un punto de acceso, que permite utilizar los equipos —netbooks y celulares— desde cualquier lugar. En las escuelas, por ejemplo, esta situación permite que los alumnos usen las computadoras del Programa Conectar Igualdad, con ubicuidad, es decir, en el aula, el patio, los pasillos, etcétera, y que estén conectados entre ellos.

Si una red no es segura, cualquier persona pueden utilizarla. Esto implica que puede utilizar parte del **ancho de banda**, y que, por lo tanto, la velocidad y la capacidad de la conexión se verán limitadas porque serán compartidas. Por otra parte, el usuario que se conecte podrá ver los sitios web visitados, los documentos en los que se trabaja y, sobre todo, los nombres de usuario y las contraseñas que se usan para registrarse en cada sitio.

Estos son algunos consejos para manejarse con seguridad en las redes inalámbricas.

- Conectarse únicamente a las redes inalámbricas que requieren una clave de seguridad o que tienen algún otro método de seguridad, como por ejemplo, un certificado.
- Antes de conectarse a una red desconocida, se debe leer atentamente la declaración de privacidad y asegurarse de que la seguridad incluye a los archivos que van a guardarse en el equipo. También hay que saber qué tipo de información recopila el proveedor de la red.
- Si se visitan sitios seguros, en los que la información está cifrada, aunque la red wifi utilizada no sea tan segura, los datos estarán protegidos. Es conveniente no quedarse conectado permanentemente a las cuentas y desconectarse al finalizar el uso.
- Si es indispensable utilizar una red wifi que no cuente con las medidas de protección citadas, es recomendable no manejar información confidencial ni ingresar contraseñas, y poner atención a las alertas para usuarios que los navegadores ofrecen.

Actividades

- Investigar la red wifi de la escuela, si la hay. Comprobar el alcance, la seguridad y la forma de funcionamiento.

Precauciones con los juegos en línea

Los juegos en línea son videojuegos en los que el usuario se conecta a internet e interactúa con dos o más jugadores que se encuentran en un sitio remoto. Muchas veces se trata de usuarios desconocidos que pueden estar en cualquier lugar del mundo.

En la actualidad, para muchos niños, jóvenes y adultos, los juegos en línea son una forma más que habitual de entretenimiento. Se puede acceder a ellos a través de varios dispositivos: la computadora, las consolas como Play Station, Wii, XBox 360, teléfonos celulares, etcétera. Según varios estudios, estos juegos, además de brindar ocio, desarrollan competencias, por ejemplo, en la resolución de problemas o la lectura de narrativas múltiples.

Sin embargo, en todos los casos, es necesario considerar que deben protegerse de ciertos riesgos. Por un lado, este tipo de juegos puede requerir la descarga de algún tipo de aplicación —aunque no es una condición necesaria—, y hay que tomar las precauciones del caso. Por otro lado, los delincuentes informáticos descubrieron en los juegos en línea una nueva posibilidad para atacar computadoras o teléfonos inteligentes.

Ingresando en una computadora a través de un juego en línea es posible:

- robar datos personales: obtener el nombre, apellido, edad, sexo, correo electrónico, contraseñas, número de tarjeta de crédito, información personal o sensible almacenada por el usuario en el dispositivo que utilice para jugar;

- *hackear* dispositivos y controlar la computadora para enviar desde allí mensajes de propaganda o virus;
- robar la cuenta de un usuario avanzado en cierto juego y "venderla" a otros que pagan por estar en un nivel adelantado;
- violar la intimidad. En ocasiones, los juegos en línea animan a los niños a hacer amistades, compartir datos de carácter personal o, incluso, reunirse con otros jugadores desconocidos fuera del juego.

Algunas de las maneras en que se vulnera la seguridad de los juegos son las siguientes:

- Se publican enlaces a sitios con la excusa de ofrecer productos y servicios o bien aportar información sobre algún tema del juego. Así se venden servicios o se obtiene información.
- Aparece —destacada en la pantalla— la invitación a instalar aplicaciones, aparentemente necesarias para poder jugar, pero con funciones inexistentes en el juego, y que, en realidad, contienen virus o propaganda.
- Se envían correos electrónicos al buzón de entrada que cada usuario tiene en el juego simulando ser la empresa que lo ha desarrollado. De esa manera, logran engañar al usuario y obtienen información sensible como datos bancarios —en el caso de los adultos—, contraseñas, información personal, etcétera.

Para trabajar en clase sobre el tema de los videojuegos, se puede consultar esta presentación: http://prezi.com/83fztudm7svw/los-videojuegos/ y la entrevista a Hernán Moraldo en el portal educ.ar: http://coleccion.educ.ar/coleccion/CD27/datos/videosjuegos_sirven_para_pensar.html [consultados el 25/03/2013].

Estas son algunas de las precauciones que es necesario tener en relación con los videojuegos en línea.

- Si requiere una aplicación, verificar si es pertinente al juego. Muchas veces aparecen más destacadas propagandas que otras aplicaciones.
- Es necesario proteger cada dispositivo vinculado con juegos en línea. Hay que tener siempre actualizadas las restricciones impuestas por el fabricante del juego, la consola u otro dispositivo. Desactivarlas elimina sus medidas de protección.
- Desconfiar de las notificaciones en las que se solicite el usuario y la contraseña y averiguar en cada caso quién —el dispositivo, la empresa que desarrolló el juego— la requiere y con qué objetivo.
- No descargar juegos de sitios no oficiales. Representan un peligro para la seguridad del jugador y de la máquina.
- Instalar y actualizar los antivirus de las computadoras, teléfonos inteligentes y otros dispositivos.
- Bajo ningún pretexto, introducir datos de tarjetas de crédito en chats.
- No olvidar que, aunque siempre se juegue en línea con los mismos usuarios, continúan siendo personas de las que desconocemos su verdadera identidad.
- Los jóvenes no deben dar datos de carácter personal a otros jugadores —nombre, dirección, etcétera—, ni aceptar reunirse a menos que cuenten con la aprobación de sus padres. Si se realiza una reunión, deberá ser en sitios públicos, con los recaudos necesarios.

Actividades

- Analizar entre toda la clase un juego en línea y observar las posibles amenazas en cada pantalla. Hacer un informe con las conclusiones.
- Realizar un video que explique cómo se juega en línea y qué cuidados hay que tomar.

Para producir un video, se puede consultar el siguiente tutorial: http://www.educ.ar/recursos/ver?rec_id=70391 [consultado el 25/03/2013].

Algunas formas de ataque a los datos personales

Hay distintas formas de ataque a los datos personales. La mayoría de ellas tiene por objetivo robar información, que luego podrá ser usada con fines publicitarios, en el mejor de los casos, o con fines delictivos, en el peor.

Phishing

El *phishing* es un término informático que se usa para denominar un tipo de delito dentro del ámbito de las estafas. En el *phishing*, el objetivo es obtener una contraseña o información detallada sobre tarjetas de crédito u otros datos bancarios. El estafador, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común este tipo de engaño se realiza mediante un correo electrónico, algún sistema de mensajería instantánea o, incluso, a través de llamadas telefónicas.

Al recibir un correo electrónico o un mensaje a través de un chat en el cual se solicite información personal financiera o de cualquier índole, no hay que responder ni hacer clic en los enlaces que aparezcan en el mensaje. Las empresas y organizaciones que trabajan dentro del marco legal —bancos, sitios de compra serios— jamás solicitan datos personales, claves o números de cuenta de sus clientes o miembros a través de correos electrónicos o mensajes.

Muchas veces, los enlaces conducen a sitios web falsos, que poseen una apariencia similar a las páginas oficiales de la organización, precisamente para propiciar el engaño.

Nunca hay que acceder a páginas web comerciales, financieras o bancarias desde un enlace que aparezca dentro del cuerpo de correo electrónico. Es preferible, si se conoce la dirección web, escribirla directamente en el navegador.

Para verificar la veracidad de un correo que solicite información confidencial, es conveniente establecer contacto con la entidad a través de información previamente conocida, como los números de teléfono de la organización.

Asimismo, muchas veces, el *pishing* ya ha sido denunciado en foros o las redes sociales. Si se coloca parte del mensaje recibido en un buscador, se podrá acceder a estas denuncias. Existen sitios en los que se registran y se difunden fraudes de este tipo, por ejemplo: http://www.antiphishing.com.ar/denuncia/.

Virus

websario

Algunos antivirus

d-Aware Free
http://www.adaware.es/

Avast! Home Edition
http://www.avast.com/index_esp.html

AVG 9.0 Free
http://free.avg.com/ww-es/homepage

Panda Active Scan 2.0
http://www.pandasecurity.com/spain/homeusers/...

Los virus informáticos, también llamados *malware*, tienen por objetivo alterar el normal funcionamiento de una computadora, sin el permiso o el conocimiento del usuario. Habitualmente, remplazan ciertos archivos por otros infectados con un código que destruye los datos almacenados en una computadora o perturba su funcionamiento. El objetivo puede ser desde una simple broma hasta causar daños significativos en los sistemas, o bloquear redes informáticas.

En el caso de las netbooks del Programa Conectar Igualdad, el ingreso de un virus perjudica al usuario del equipo y, si los equipos están en red, a toda la institución educativa. Se pueden perder materiales, trabajos de los alumnos o dificultar el uso normal de los equipos.

El nivel de peligrosidad de los virus se establece en función de los daños que es capaz de producir en el sistema. Algunos virus simplemente envían mensajes, mientras que otros destruyen archivos y programas.
Toda computadora —así como la red escolar— tiene que tener un sistema antivirus actualizado. Esto permite detectar y desactivar los ataques. En la actualidad, existen numerosos sitios públicos donde se puede encontrar información sobre los virus y cómo prevenir sus ataques. Por ejemplo: http://www.convosenlaweb.gob.ar/padres/amenazas.aspx [consultado el 25/03/2013].

Pharming

Pharming es un delito que consiste en cambiar la dirección de dominio de un sitio, para pasarla a otra máquina. De esta manera, se hace creer al usuario que el sitio visitado es el original, cuando en realidad es una copia. El usuario vuelca información personal, creyendo que es una página de confianza, y sus datos van a parar a otras manos. Si se va a volcar información personal en un sitio, es conveniente chequear la dirección, ingresando por la barra de direcciones del navegador y no desde un enlace.

Algunos buscadores tienen herramientas para testear sitios y comprobar su seguridad. En las últimas versiones de Internet Explorer, por ejemplo, en el menú principal, en “Propiedades”, existe la opción “Certificados”, que chequea la legitimidad del sitio; el explorador Mozilla tiene un *Testpharming* que se puede descargar. También es importante utilizar un proveedor de internet confiable, que publique información sobre sitios peligrosos, avise de posibles amenazas y proteja sus propios servidores. Para esto, se pueden hacer las consultas pertinentes al proveedor.

Troyanos

Los troyanos están diseñados para permitirle a un individuo el acceso remoto a un sistema o equipo. El troyano es un archivo que se introduce en un equipo y se puede manejar desde otro. Para ello, se presenta como un programa legítimo e inofensivo. Un troyano puede estar ejecutándose en una computadora durante meses sin que el usuario perciba nada.

Algunas de las operaciones que se pueden llevar a cabo desde la máquina en la que se aloja son:

- realizar ataques de denegación de servicio o envío de *spam*;
- instalar otros programas, incluyendo otros programas maliciosos;
- robar información personal: datos de las cuentas bancarias, contraseñas, códigos de seguridad;
- borrar o transferir archivos.

Estos son algunos de los recaudos que se pueden tomar para evitar el ataque de este tipo de programas maliciosos.

- Disponer de un programa antivirus actualizado regularmente, para estar protegido contra las últimas amenazas.
- Disponer de un *firewall* —o cortafuegos— programado para filtrar los sitios incorrectamente configurados. Algunos antivirus lo tienen incorporado.
- Tener instaladas las últimas actualizaciones de seguridad del sistema operativo.
- Descargar los programas de páginas web oficiales o de sitios de confianza.
- No abrir los datos adjuntos de un correo electrónico si se desconoce el remitente.
- Prestar atención si un programa desconocido se ejecuta al iniciar la computadora, se crean o se borran archivos de forma automática, hay errores en el sistema operativo o la computadora funciona más lento de lo normal.

Keyloggers

Los *keyloggers* son programas que se introducen en un equipo y registran las pulsaciones que se realizan en el teclado. Posteriormente, las graban en un archivo y las envían a través internet. De esta manera, otros usuarios acceden a contraseñas, números de una tarjeta de crédito u otro tipo de información personal de manera ilícita.

Tener instalado un programa del tipo *anti-spyware* o un monitor de red que pueda detectar diversos *keyloggers* y limpiarlos.

Sidejacking

+ Información

Con vos en la web, Dirección Nacional de Protección de Datos Personales. Recuperado de http://www.convosenlaweb.gob.ar/padres/amenazas.aspx

El *sidejacker* espía y copia la información contenida en las *cookies* de una máquina conectada a la misma red, y así accede a las cuentas de la víctima. Esta modalidad de ciberataque suele darse en lugares públicos en donde hay redes wifi, que comparten la misma conexión a internet. Al compartir la red, el atacante se introduce en la computadora de la víctima, toma posesión de sus *cookies* y así accede a información sobre cuentas, claves, etcétera.

Hay que evitar el uso de claves o contraseñas personales al utilizar redes públicas.

Gusanos

Los gusanos se presentan como un programa aparentemente legítimo e inofensivo, pero al ejecutarlos ocasionan daños severos. En general, los gusanos se instalan cuando el usuario descarga programas o aplicaciones de fuentes no confiables.

- No instalar software que proceda de una fuente poco fiable. Es recomendable utilizar los servicios de descarga del fabricante o los sitios autorizados para la obtención de nuevas versiones y actualizaciones de los programas.
- Actualizar el antivirus, el software de seguridad y el sistema operativo periódicamente.
- No abrir correos de remitente desconocido. Podrían contener enlaces o archivos nocivos para la computadora.

websario

La configuración de privacidad en los principales buscadores

Internet Explorer
http://download.live.com/familysafety

Google
http://www.google.com.ar/preferences?hl=es

Bing
http://www.bing.com/settings.aspx?ru=%2f&FORM...

Yahoo!
http://ar.search.yahoo.com/preferences/prefer...

La información privada en las redes sociales

Las redes sociales son los espacios en los que los jóvenes publican la mayor cantidad de información. El trabajo con los alumnos sobre el tema de la privacidad en estos entornos se debe encarar en dos grandes líneas. Por un lado, es posible ajustar la configuración de las cuentas y activar las medidas de privacidad y seguridad más estrictas. Así, se delimita el acceso a los datos para que sean accesibles solamente a quienes el usuario desea. Por otro lado, se deben realizar actividades de reflexión sobre el tipo de información personal y de otras personas que se publica cuando se hace una afirmación al pasar, se publica una fotografía o un video.

Facebook es la red social más popular en todo el mundo. Millones de usuarios están conectados a través de sus perfiles. Así, cualquiera que ingrese un nombre podría tener acceso a ese perfil. Al menos, a la información que es pública por defecto (*default*). Por eso, es importante activar las opciones de configuración de privacidad para determinar qué tipo de información se quiere mostrar. Esta configuración permite bloquear el acceso a los datos, para que solamente sean vistos por los "amigos". Así, es posible asegurarse de que las fotos, videos, publicaciones, gustos e intereses solo sean conocidos por quienes cada uno desea.

En Twitter la cuestión de la intimidad y privacidad es distinta, porque no se trata realmente de una red social, sino más bien de una red de información: los usuarios "siguen" a otros por los tuits que estos envían, escribiendo y opinando sobre determinado tema. En Twitter las fotos o videos pasan a un segundo plano. Importa mucho más la instantaneidad de los mensajes que los datos personales. De todas maneras, se pueden proteger los tuits para que solo sean vistos por quienes los usuarios autorizan. Así, la información personal no llega a desconocidos.

"Pensar antes de publicar" es un video realizado por varias organizaciones de los Estados Unidos para concientizar sobre internet como espacio público. Recuperado de http://www.youtube.com/watch?v=2qR8uSyTZH0 [consultado el 26/03/2013].

"Hay que pensar las redes sociales como la plaza pública: un lugar de encuentro, que ofrece muchas más posibilidades que el chat. La inclusión de imágenes, por ejemplo, es muy significativa en esta época, y para los adolescentes en particular. Por supuesto que hay otras cuestiones que tienen que ver con la posibilidad de armar grupos de interés, la pertenencia, la identidad. Las redes sociales son una plaza pública para estar, pero que permite diferentes modos de estar. Y esto se vuelve funcional al continuar la vida por fuera de internet".

Entrevista a Sergio Balardini, recuperado de http://bibliotecadigital.educ.ar/articles/read/283 [consultado el 26/03/2013].

Actividades

- En el siguiente enlace (http://www.educ.ar/recursos/ver?rec_id=109154), es posible encontrar una nota publicada en el portal educ.ar en la que se desarrolla el tema de las redes sociales como espacios para construir un PLE (entorno personal de aprendizaje), es decir, un conjunto de contactos profesionales, académicos y educativos para estar informados.
  La nota está enfocada a docentes, pero es posible realizar con los alumnos un trabajo similar. Reflexionar sobre a quiénes siguen o tienen de amigo en las redes sociales y por qué, a quiénes podrían vincularse para estar informados sobre temas académicos, a quiénes deberían borrar o limitar, etcétera.

websario

Configuraciones de privacidad en las redes sociales más populares

Facebook
http://www.youtube.com/watch?v=_-qD_BjXWgk&list=UU4sslkrtCl8hcmf93NawZUQ&index=2

Twitter
http://www.youtube.com/watch?v=8Q03Ov_VMp8&list=UU4sslkrtCl8hcmf93NawZUQ&index=14

Youtube
http://www.youtube.com/watch?v=kCZWlVUrQ0k&list=UU4sslkrtCl8hcmf93NawZUQ&index=13

Referencias bibliográficas y sitios de consulta

Referencias bibliográficas

AA. VV.: *La generación interactiva en la Argentina*, Buenos Aires, Fundación Telefónica, 2008.

Bacher, Silvia: *Tatuados por los medios*, Buenos Aires, Paidós, 2009.

Balardini, Sergio: "Qué hay de nuevo, viejo", en Nueva Sociedad, N° 200, Santiago de Chile, CEPAL, 2005. Disponible en: http://www.nuso.org/upload/articulos/3299_1.pdf.

Jenkins, Henry: *Building the Field of Digital Media and Learning*, Chicago, McArthur Fundation, 2009.

Jenkins, Henry: *Fans, blogueros y videojuegos*, Barcelona, Paidós, 2009.

Tabachnik, Silvia: *Lenguaje y juegos de escritura en la red*, México, Universidad Autónoma Metropolitana, 2012.

Sitios de consulta

Educ.ar, Ministerio de Educación: *Cuando estás conectado*. Recuperado de http://bibliotecadigital.educ.ar/articles/read/283

Educ.ar, Ministerio de Educación: *Uso responsable y seguro de TIC*. Recuperado de http://coleccion.educ.ar/coleccion/CD27/inicioCD27.html

Dirección Nacional de Protección de Datos Personales, Ministerio de Justicia y Derechos Humanos: *Con vos en la web*. Recuperado de http://www.convosenlaweb.gob.ar/

Jefatura de Gabinete de Ministros, Presidencia de la Nación: *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*. Recuperado de http://www.icic.gob.ar/paginas.dhtml?pagina=100

Jefatura de Gabinete de Ministros, Presidencia de la Nación: *Prevención en el uso de redes sociales*. Recuperado de http://www.youtube.com/watch?v=Nrmz0wKC1i0&lr=1&user=JGMgovar&feature=iv&annotation_id=annotation_470540

Programa Escuela y Medios, Ministerio de Educación: *Internet en Familia*. Recuperado de http://coleccion.educ.ar/coleccion/CD27/datos/internet_familia_1.html.

Algunos títulos de la colección

Serie para la enseñanza en el modelo 1 a 1

- Aritmética
- Arte
- Artes visuales
- Biología
- El bibliotecario escolar en el modelo 1 a 1
- Ética
- Física
- Física 2
- Formación Ética y Ciudadana
- Geografía
- Geografía 2
- Geometría
- Inglés
- Lengua
- Lengua 2
- Portugués
- Química
- Química 2

Serie computadoras portátiles para las escuelas de educación especial

- Inclusión de TIC en escuelas para alumnos con discapacidad intelectual
- Inclusión de TIC en escuelas para alumnos con discapacidad motriz
- Inclusión de TIC en escuelas para alumnos con discapacidad visual
- Inclusión de TIC en escuelas para alumnos sordos

Serie estrategias en el aula para el modelo 1 a 1

- El modelo 1 a 1: notas para comenzar
- Cursos virtuales
- Juegos
- Investigación, gestión y búsqueda de información en internet
- Comunicación y publicación
- Mapas conceptuales digitales
- Producción multimedia (videos y animaciones)
- Trabajos colaborativos
- Simulaciones

Serie instrumental para el modelo 1 a 1

- Sistemas operativos en las netbooks: GNU/Linux y Microsoft Windows

Serie gestión educativa en el modelo 1 a 1

- El modelo 1 a 1: un compromiso por la calidad y la igualdad educativas
  La gestión de las TIC en la escuela secundaria: nuevos formatos institucionales
- Manual de gestión con el modelo 1 a 1

Serie familias

- La computadora en casa

Especiales

- Estrategia político pedagógica y marco normativo del Programa Conectar Igualdad
- Múltiples voces para el bicentenario

ARGENTINA
UN PAIS CON BUENA GENTE