La última década del siglo XX y los primeros años del siglo XXI están signados por la apertura y la generalización del uso de las nuevas tecnologías de la información y la comunicación. Y especialmente en los últimos años, la www se ha afirmado como un espacio virtual de intercambio de información privilegiado. Las consecuencias de estos cambios pueden verse en diversos campos y temas. En el presente capítulo trataremos de plantear las cuestiones más candentes. ¿A quién pertenece la información? ¿Quiénes tienen derecho a conocerla? ¿Qué diferencia lo público y lo privado? ¿Cómo hacer para que más gente tenga acceso a más información y garantizar un acceso democrático a la información? Se adelantarán algunas respuestas junto con los argumentos más destacados. Pero es importante advertir que se trata de problemáticas sumamente actuales, vigentes y dinámicas, por lo que resulta recomendable profundizar cada tema en otras fuentes para llegar a una toma de posición equilibrada.

CAPÍTULO 9

¿Y más allá?

Miscelánea y nuevos escenarios

- **Salud y nuevas tecnologías.**
  Posibles consecuencias sobre la salud.
- **Ciberespacio como ámbito de interacción y confrontación. Libertad y control.**
  Lo propietario y lo libre.
- **Seguridad y protección.**
  Privacidad.
  El Gran Hermano en 1984.
  Criptografía.
  Ética del hacker y libertad del conocimiento.
  Virus.
  Los *hoax*.
- **Compartir archivos.**
- **Los estados Nacionales y la utilización del *software* libre.**
  El caso del Perú.
  ¿En el futuro se votará de manera electrónica?
- **Un paso más allá. El futuro que está por llegar.**
  ¿Podrán pensar las máquinas?
  Inteligencia artificial.
  Realidad virtual.
  ¿Triste y solitario final para los libros?
  ¿Pueden las máquinas tomar decisiones?
  Violencia y videojuegos.
- **Reflexiones finales.**

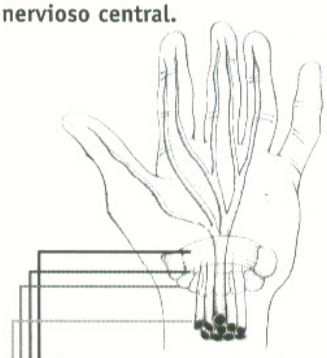
Salud y nuevas tecnologías

¿Qué es el Síndrome del Túnel Carpiano?

Se trata de la hinchazón de los tendones que se encuentran alrededor de los carpos, que conforman algo similar a un túnel, como se ven en la ilustración. Es una enfermedad de trauma acumulativo, al flexionar y extender la muñeca repetitivamente, la cubierta protectora que rodea cada tendón se inflama y hace presión sobre el nervio mediano.

Los síntomas van desde una sensación de hormigueo doloroso en la/s mano/s durante la noche, pasando por una sensación de inutilidad de los dedos y de hinchazón, mayor a la que se ve. Puede llegar a una disminución sensible de fuerza y habilidad con las manos.

Información desde la mano al sistema nervioso central.



Ligamento transversal carpiano: El ligamento que conecta los huesos carpos completando el "túnel".
El túnel carpiano: Los ocho huesos y el ligamento forman el túnel por el que pasan tendones y el nervio mediano.
Huesos carpos: Ocho huesos que forman una U en la base de la palma.
Tendones flexores: Nueve pequeños tendones que pasan a través del túnel y permiten los movimientos de los dedos.

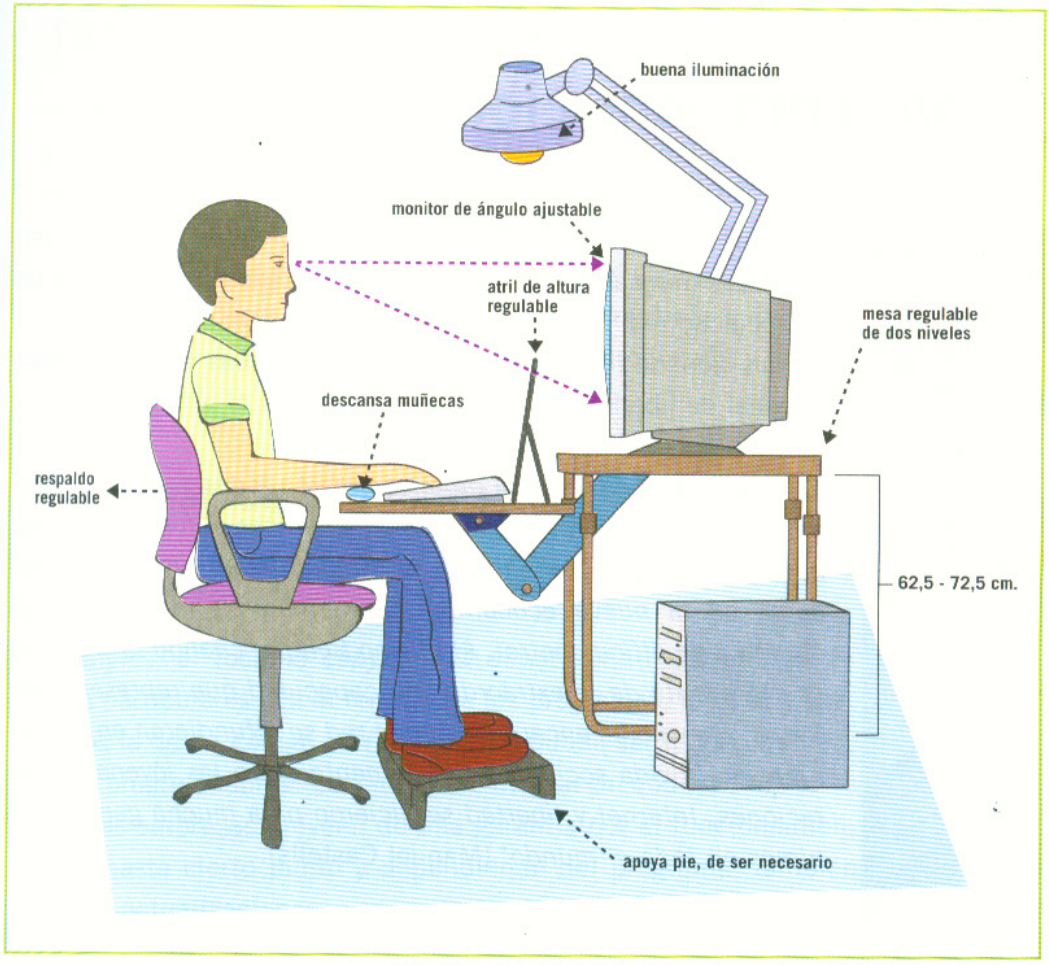
La utilización de las nuevas tecnologías ha transformado y facilitado la manera de ejecutar todo tipo de acciones, pero también ha traído aparejados algunos problemas de salud, relacionados con el uso de la PC. En algunos casos se deben al uso incorrecto de la computadora, como la adopción de malas posturas, y en otros, a cuestiones intrínsecas de la herramienta, como por ejemplo, el parpadear imperceptible de los monitores, que produce cansancio, molestias oculares y dolores de cabeza. Estar mucho tiempo sentados frente a una computadora, tiene habitualmente las siguientes características:

- Falta de movimiento.
- Bajo nivel de exigencia cardiorrespiratoria.
- Fijación de la mirada a corta distancia y durante largo tiempo.
- Posturas ineficientes, de alto gasto energético y reiteradas en el tiempo.
- Tensión sostenida en manos y miembros superiores por uso intensivo y/o inadecuado del teclado o el mouse.
- Aislamiento, excesiva concentración, estrés (efecto hipnótico).
- Disminución de la capacidad de registro y percepción de la postura y la conciencia corporal.

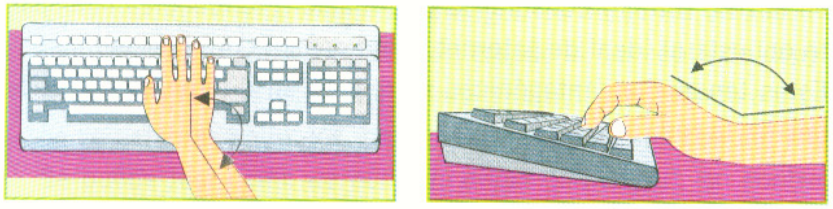
Fuente: http://www.saludypc.com

Posibles consecuencias sobre la salud

Las consecuencias están registradas en múltiples estudios de las distintas áreas de la salud: fatiga, irritabilidad, cefaleas, mareos, trastornos circulatorios y neurovegetativos (sistema nervioso autónomo), cansancio visual, picazón o ardor de los ojos, lagrimeo, dolor e irritación ocular, dolores, contracturas musculares, hormigueos (en las manos, en los brazos, hombro, cuello y otras zonas), síndrome del túnel carpiano, tendinitis y otros.



Postura correcta para trabajar en la computadora.



La postura de la muñeca que produce el Síndrome del Túnel Carpiano.

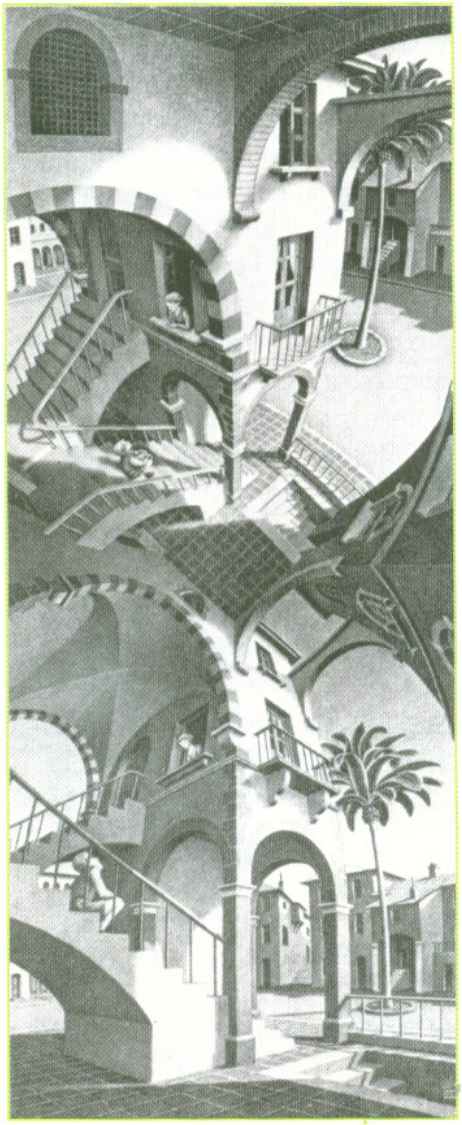
Actividad 9.1.

Consejos para la salud

Les proponemos que realicen un estudio de campo en el entorno más cercano. Diseñen una encuesta que contemple estos aspectos presentados. ¿Qué preguntas harían? ¿Cómo organizarían la información obtenida?

A partir de las conclusiones, diseñen folletos para difundir la información y proponer cuidados para la prevención de la salud de los usuarios.

Ciberespacio: ámbito de interacción y confrontación. Libertad y control



Litografía "Arriba y abajo" de M. C. Escher - 1947.

El ciberespacio es un ámbito de interacción social, donde se ven reflejadas muchas de las confrontaciones, tensiones, e ideales de la "sociedad real".
Por un lado, se reconocen los valores de quienes ven en Internet un ideal de libertad:

"Los valores libertarios de quienes crearon y desarrollaron Internet, a saber, los investigadores académicos informáticos, los hackers, las redes comunitarias contraculturales y los emprendedores de la nueva economía, determinaron una arquitectura abierta y de difícil control. Al mismo tiempo, cuando la sociedad se dio cuenta de la extraordinaria capacidad que representa Internet, los valores encarnados en la red se difundieron en el conjunto de la vida social, particularmente entre las jóvenes generaciones. Internet y libertad se hicieron para mucha gente sinónimos en todo el mundo" (Manuel Castells).

Por el otro lado, hay una tendencia hacia el control, hacia la vigilancia, que se expresa en el desarrollo de tecnologías que permiten recolectar información sobre la actividad de los usuarios en la red, filtrar y censurar la información, tendencia claramente opuesta al ideal de Internet como espacio de libertad.
Estas tendencias antagónicas se relejan en diferentes expresiones en la red.

Lo propietario y lo libre

Propiedad del código fuente

En los comienzos de Internet, los programadores exponían los códigos fuente de los programas para que cualquiera pudiera analizarlos, modificarlos y mejorarlos (ver **Capítulo 6**). Desde la década del 90 comenzaron a proliferar empresas que desarrollan programas manteniendo los códigos resguardados. En la actualidad hay diversos argumentos para cuestionar esta práctica: legales, éticos, políticos y filosóficos.

Uno de ellos promueve un debate muy interesante sobre la naturaleza del código de los programas, y si es legal mantener el secreto del código, pues si se lo trata como conocimiento que regula la vida social, mantener el secreto impide que sea discutido públicamente. Desde este punto de vista, el código fuente funciona como una "constitución" del ciberespacio, en cuyo caso debería estar disponible para las revisiones y modificaciones. En lo que respecta al *software* libre, este escrutinio público es posible, además de las ventajas de la libre circulación y progreso por obra de la colaboración comunitaria.

Para estar al tanto de cuestiones importantes sobre las diferencias entre lo propietario y lo libre:
http://www.cibersociedad.net/archivo/articulo.php?art=39

Propiedad de la información

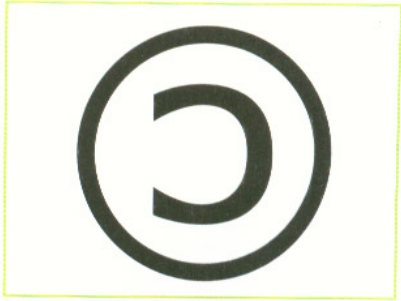
Copyright

En inglés, el vocablo ***copyright*** © denota una reserva de derechos particulares. En el terreno de los programas, la consecuencia es la de un código cerrado que no puede ser modificado por otros programadores. La ventaja de utilizar un código cerrado es que las empresas proveen de una garantía por el funcionamiento y, hasta cierto punto y dependiendo del programa, también de las actualizaciones.

Copyright (del *Diccionario de Uso de la lengua española,* de María Moliner): Palabra inglesa con la que se consigna en los libros, generalmente en la anteportada, el hecho de estar registrado y garantizado el derecho exclusivo de su reproducción, con la expresión de la fecha y la persona o la entidad en favor de la cual se establece ese derecho. * (masc.). Esa consignación: 'El *copyright* es de 1958'.

Copyleft

En oposición a este modo de proteger los derechos de autor, los impulsores del *software* libre han creado el concepto de ***copyleft*** (quien propuso la idea fue Richard Stallman), apelando a un juego de palabras en inglés, para marcar la oposición con *copyright*. Se puede leer como *derecho de copia* (*copyright*), en contraposición a *copia que se deja o se permite* (*copyleft*), y apela también a la oposición lateral derecha *(right)*-izquierda *(left)*.
El planteo de una licencia libre no significa dejar a su suerte al programa, pues si éste fuera el caso, cualquier empresa podría publicarlo como propio, o bien hacer alguna pequeña modificación, "cerrar" el código y venderlo como propio.
Por eso es que fue creada la licencia GNU (que quiere decir "*no es Unix*"), con las siguientes características: se pone el *software* bajo *copyright* y se ofrece una licencia, que da permiso legal para acceder al código fuente, lo que habilita a copiar, distribuir y/o modificar el *software*.



Copyleft.

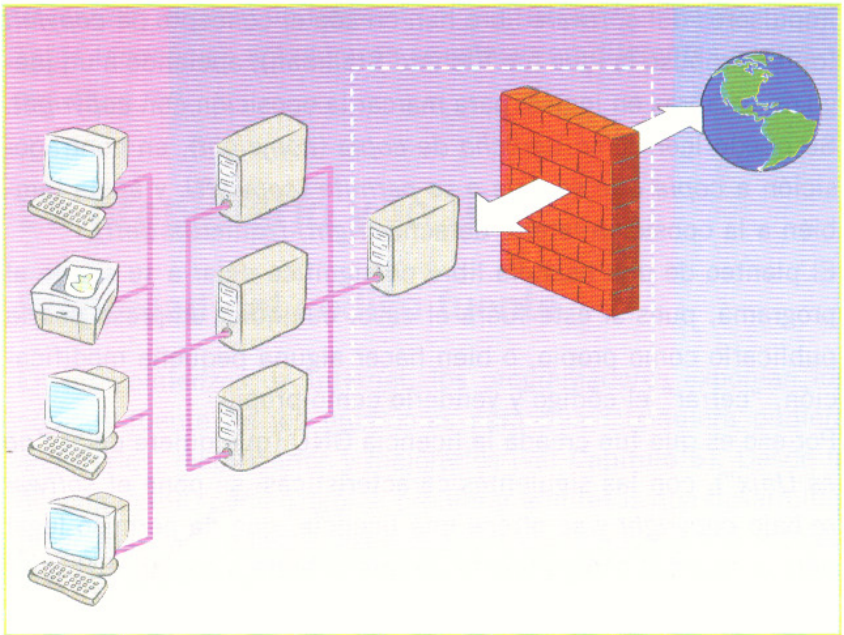
Seguridad y protección

En informática, estos conceptos aluden a la creación de plataformas o programas que puedan impedir que usuarios o programas ejecuten acciones no permitidas por el sistema. Por ejemplo, el acceso a determinada información.

Una dificultad consiste justamente en permitir que los usuarios legítimos realicen determinadas acciones, mientras se les impide lo mismo a otros usuarios no autorizados.

Entre los programas utilizados para la protección cabe mencionar:

- los programas **antivirus**: diseñados para detectar o impedir la entrada de programas infectados.
- los **antiespías** *(antispyware)*: evitan que algún programa o persona sepa qué estamos haciendo con nuestro equipo o cómo nos conectamos con los diversos sitios, etcétera.
- Los **cortafuegos** (tomado del concepto en inglés *firewall*): se trata de filtros que impiden el paso de paquetes de información que no cumplan con los criterios determinados por la administración de una red, y sí permiten el paso de paquetes de información cuyas características están previstas por el sistema. Existen en dos niveles: para los usuarios de computadoras personales, que impiden las intrusiones, y para las computadoras que conectan redes entre sí. El objetivo general es el mismo, filtrar el tráfico indeseado.



Gráficos que representan el funcionamiento de los "*firewall*", verdaderas murallas de contención de información no deseada.

En la actualidad, las empresas que producen programas vinculados a la seguridad, están empezando a ofrecer suites de programas que realizan todas las rutinas de seguridad: antivirus, *firewall*, *antispam*, *antispyware*, y la eliminación de las ventanas publicitarias que se abren sin consentimiento de los usuarios (*pop ups*).

Privacidad

La privacidad se ha convertido en un tema de suma importancia en la Sociedad de la Información. Aunque en siglos anteriores tuvo su importancia, el nivel de exposición y de intrusión en la vida privada de las últimas décadas es muchísimo mayor.

Lo paradójico es que los diversos modos de recolección de información sobre los usuarios o las organizaciones están hechos para dar mejores servicios o para proteger a los usuarios. Sin embargo, también se han convertido en una forma de vigilar la conducta de los ciudadanos.

Muchísimas veces, esta información se recolecta con el consentimiento de los usuarios, como en el caso de los documentos de identidad, pasaportes, encuestas, etc., dado que en general se asume que la vida en sociedad está relacionada con cierta renuncia a algunas libertades individuales. Pero otras veces, esto se realiza a espaldas de los ciudadanos, sea a través del registro de los hábitos de compra en los supermercados o del control del correo electrónico, por ejemplo.

En Internet es posible recolectar información sobre los hábitos de navegación de un usuario determinado. Esto se lleva a cabo instalando una clase de programas llamados ***spyware***, sin el consentimiento del usuario, cuya función es registrar todas las acciones que se realizan en Internet, y luego enviar los datos recolectados a una gran base de datos.

En el apartado **Seguridad y protección** profundizamos acerca de este tipo de programas "invasivos".

El movimiento de los ciudadanos es diariamente registrado en cámaras ubicadas en diferentes partes de la ciudad.

Metáfora del *spyware*.

El Gran Hermano en 1984

En el año 1946, **George Orwell** escribió una de sus novelas más conocidas e impactantes: *1984*. Una película inglesa basada en esta novela se estrenó en Argentina bajo el título de *Premonición 1984*. La novela refleja un futuro dominado por una dictadura totalitaria omnipresente que controla todos los momentos de la

George Orwell (1903-1950).

"Quien controla el pasado, controla el futuro. Quien controla el presente, controla el pasado"

George Orwell, *1984*.

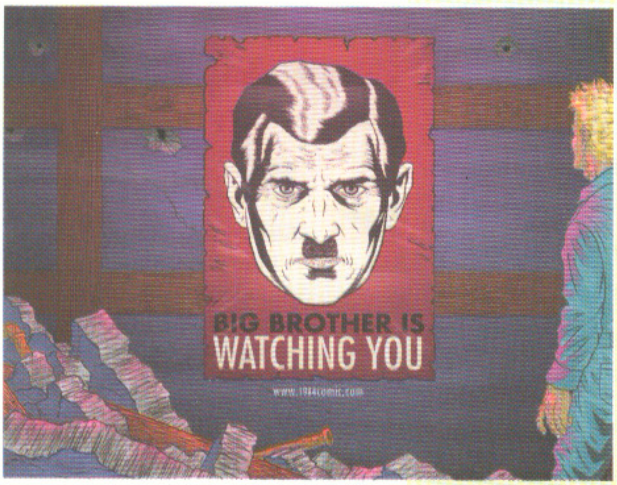
1984: Los tres lemas del Partido

La guerra es la paz.
La libertad es la esclavitud.
La ignorancia es la fuerza.

George Orwell: "1984".

vida de los ciudadanos. El protagonista, Winston Smith, vive en una ciudad dominada por el Gran Hermano (del inglés: *Big Brother*) y con un partido único (crítica atribuible a toda dictadura). En la novela se plantean también varias estrategias de la acumulación de poder, como la modificación de los registros periodísticos, procedimiento con el que se altera la memoria de la humanidad.

La actualidad de los planteos de Orwell es impresionante, pues los avances tecnológicos han permitido que los gobiernos posean una gran capacidad de procesamiento de datos y seguimiento de actividades. Por ejemplo, resulta posible "revisar" el tráfico de correo electrónico en busca de una determinada secuencia de palabras, la cantidad de cámaras puestas sin aviso por doquier: bancos, centros de compras, supermercados, aeropuertos e instituciones de diverso tipo constituyen una pequeña muestra de la aplicación de la tecnología a la vigilancia ciudadana.



Portada de distintas ediciones de la novela "1984".

Placa conmemorativa, situada en la esquina de Pond Street y South End Green, Londres. Allí funcionaba la librería donde trabajó entre 1934 y 1935.

Actividad 9.2.

Construyendo personajes

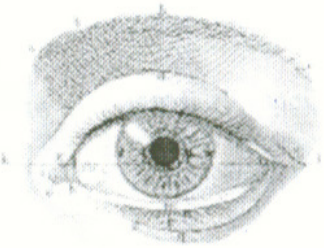
Intenten un recorrido imaginario por alguna ciudad. Registren todas las situaciones y lugares en los que es posible observar la conducta de los ciudadanos.

Siguiendo con la ficción, construyan una breve historia caracterizando a cada uno los personajes observados. Por ejemplo: Raúl Costa trabaja en las Torres de la calle Leandro Alem. Entra a las 10 y sale entre las 18 y las 20. Opera en el Banco XXX y semanalmente retira dinero del cajero. Reservó dos boletos de avión a Porto Alegre para enero. Es fanático de las películas de suspenso que alquila todos los viernes en el video cercano a su domicilio, etcétera.

Si quieren pueden formar dos grupos: los que definen a los personajes y los que, a partir de estas definiciones, los incorporan a las historias.

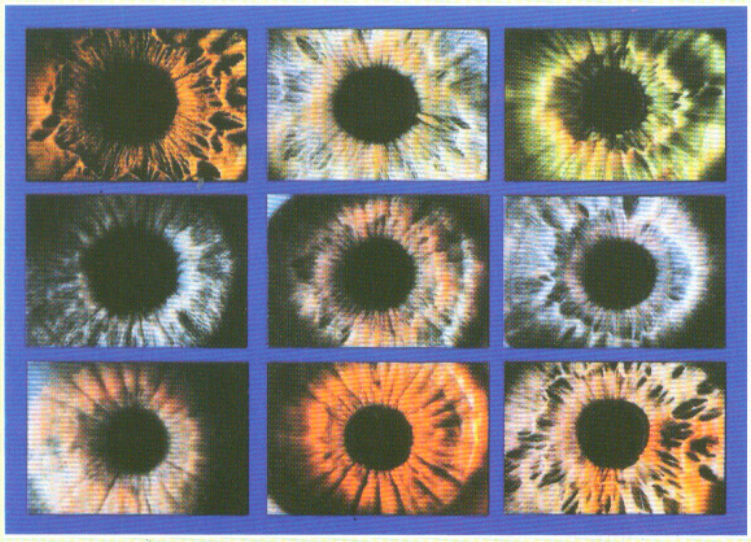
El debate sobre la vigilancia electrónica

En la actualidad, diferentes organizaciones poseen información sobre los ciudadanos en sus bases de datos: los bancos sobre los movimientos de dinero; las tarjetas de crédito, sobre los hábitos de consumo; el sistema de salud, sobre las enfermedades y estudios realizados y la medicación que se consume; de la misma manera, la información sobre licencia de conducir, infracciones de tránsito, historia escolar, reserva de boletos de viaje...; todo ello se encuentra archivado. En general no existe comunicación entre las diferentes agencias, por lo que cada una posee un registro fragmentado del perfil de cada ciudadano. ¿Pero qué pasaría si existiera la voluntad de recopilar toda la información disponible sobre los ciudadanos en una única base de datos? ¿Quién podría tener acceso a esta información? ¿Qué uso se le podría dar? ¿Cómo proteger la información personal e íntima? ¿Recopilar información personal es una violación de las libertades cívicas? Una de las preguntas más actuales en muchos países es: ¿Hasta dónde los motivos de seguridad y de lucha contra el terrorismo justifican la invasión de la intimidad de los ciudadanos?



Biometría

La *biometría* consiste en la identificación de los individuos a partir de sus características físicas (huellas dactilares, iris, forma de la mano y de la cara). Esta disciplina ha cobrado un gran avance a partir de la posibilidad de la digitalización y tratamiento automático de los datos.



Digitalización de imágenes de iris:
http://www.cl.cam.ac.uk/users/jgd1000/iriscollage.jpg

Digitalización
de una huella dactilar.

Criptografía

Algunas direcciones de Internet se inician con el nombre del protocolo **https**, donde la **s** señala que se trata de un protocolo http con niveles de seguridad mayores para permitir la privacidad en el intercambio de datos.

La **criptografía** (del griego *kryptós*, "oculto", y *gráphein*, "escritura") es el estudio que se ocupa de transformar la información de manera que sólo pueda ser leída por aquellos a quienes está dirigida. Originalmente el uso de la criptografía estaba más o menos restringido a usos militares o gubernamentales. Pero con el advenimiento y la generalización de Internet, este uso se ha expandido a usuarios particulares, pues, en rigor, la mayor parte de las comunicaciones entre computadoras, correo electrónico, etc., se realiza de modo transparente. Por ejemplo, el correo electrónico es equivalente a enviar postales, es decir, sin sobre cerrado. En este caso, los paquetes de información pueden ser interceptados y reconstruidos, y así obtener el contenido de las comunicaciones de una persona. También resulta posible monitorear el intercambio de archivos que se realiza cuando se los "sube" a una página web.

Por todos estos aspectos mencionados ya existen protocolos para intercambiar archivos en forma segura con los servidores de una página web, sea ésta personal, de un banco, una empresa, etc. En el caso de los bancos, este tema resulta especialmente crítico, pues de esas medidas de seguridad dependen las cuentas de muchísima gente.

Los defensores de la libertad absoluta en la red sostienen que la criptografía es una tecnología fundamental para permitir la libertad en la red. Aunque como todas las tecnologías (ver **Capítulo 2**) su relación con criterios éticos puede ser ambigua. Si bien puede permitir que el ciudadano bienintencionado proteja su privacidad, también es posible que esta tecnología sea utilizada por organizaciones terroristas, a fin de comunicarse libremente. El tema sobre la tecnología de encriptación está en un profundo debate. Algunos gobiernos, con el argumento de la seguridad y prevención del terrorismo, han prohibido la exportación de la tecnología de encriptación.

Criptología. Breve introducción

Desde que el hombre ha necesitado comunicarse con los demás, ha tenido también la necesidad de que algunos de sus mensajes sólo fueran conocidos por las personas a quienes estaban destinados. La necesidad de poder enviar mensajes de forma que sólo fueran entendidos por los destinatarios hizo que se crearan **sistemas de cifrado**, de forma tal que un mensaje después de un proceso de transformación, al que llamamos cifrado, solo pudiera ser leído siguiendo un proceso de descifrado. Las civilizaciones más antiguas (egipcia, mesopotámica, china) ya usaban esos métodos.

Uno de los primeros métodos de encriptado que está documentado es atribuido a Julio Cesar, y se basaba en la sustitución de las letras de un documento por la tercera letra que le correspondiese en el alfabeto. Así la A se convertía en una D, la B en E ...

Con el tiempo y debido principalmente a su uso militar, los sistemas criptográfícos fueron haciéndose cada vez más complejos, hasta llegar a nuestros días, en que la informática ha entrado en nuestras vidas y la necesidad de seguridad al realizar nuestras operaciones ha aumentado considerablemente.

Cómo funciona

Una rama de la criptología es la criptografía, que se ocupa del cifrado de mensajes. Esta se basa en que el emisor emite un mensaje en claro, legible, que es tratado mediante un cifrador con la ayuda de una clave, para crear un texto cifrado. Este texto cifrado, por medio del canal de comunicación establecido, llega al descifrador, quien convierte el texto cifrado, apoyándose en otra clave, para obtener el texto en claro original. Las dos claves implicadas en el proceso de cifrado/descifrado pueden ser o no iguales, dependiendo del sistema de cifrado utilizado.

Sistemas de cifrado

Sistemas de cifrado simétrico

Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto, se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave.

Es importante que dicha clave sea muy difícil de descifrar ya que hoy en día los ordenadores pueden obtener las claves muy rápidamente. Por ejemplo, el algoritmo de cifrado DES usa una clave de 56 bits, lo que significa que hay 72 mil billones de claves posibles. Actualmente ya existen ordenadores especializados que son capaces de probar todas ellas en cuestión de horas.

Hoy por hoy se están utilizando ya claves de 128 bits que aumentan el "espectro" de claves posibles (2 elevado a 128), de forma que aunque se uniesen todos los ordenadores existentes en este momento, no lo conseguirían ni en miles de millones de años.

Sistemas de cifrado asimétrico

También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella.

Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, y ni siquiera quien ha cifrado el mensaje puede volver a descifrarlo.

Por ello, se puede dar a conocer perfectamente la clave pública, para que todo aquel que se quiera comunicar con el destinatario pueda hacerlo.

Sistemas de cifrado híbridos

Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente, por lo que, si un atacante pudiera descubrir la clave simétrica, solo le valdría para ese mensaje y no para los restantes.

Tomado de: http://seguridad.internautas.org/criptografia.php

Fragmento del *Criptonomicón*, de **Neal Stephenson.**

...Randy arranca un programa que técnicamente se llama Novus Ordo Seclorum pero que todo el mundo abrevia como Ordo. Es un chiste muy forzado que se fundamenta en que la tarea de Ordo, como programa criptográfico, consiste en colocar los bits en un Nuevo Orden y le llevaría siglos al gobierno descifrarlo. En medio de la pantalla aparece la imagen de la Gran Pirámide, y un solitario ojo se materializa gradualmente en su ápice.

Ordo puede realizar su trabajo de dos formas. La más evidente es descifrar todos los mensajes y convertirlos en archivos de texto en el disco duro, que Randy podría leer en cualquier momento (página 42)

(...)
Avi le envió un mensaje de correo cifrado:

Cuando llegues a Manila me gustaría que generases un par clave de 4096 bits y lo guardes en un disco floppy que lleves encima todo el tiempo. No la conserves en tu disco duro. Cualquiera podría entrar en tu habitación cuando no estés y robar la clave.

Ahora Randy despliega un menú y elige el elemento etiquetado como «Nueva clave...».
Se le ofrecen varias opciones para LONGITUD DE LA CLAVE: 768 bits, 1024,1536,2048, 3072, u Opcional. Randy elige la última opción y luego, con cansancio, teclea 4096.

Incluso romper una clave de 768 bits requiere vastos recursos. Si se añade un bit, para hacerla de 769 bits, el número de claves posibles se duplica, y el problema se vuelve mucho más difícil. Una clave de 770 es aún más difícil, y así sucesivamente. Usando claves de 768 bits, Randy y Avi podrían mantener sus conversaciones en secreto para casi todas las entidades del mundo durante los próximos años. Una clave de 1024 bits sería astronómicamente más difícil de romper.

Algunas personas llegan al punto de usar claves de 2048 e incluso 3072 bits de longitud. Eso detendría a los mejores descifradores del mundo durante periodos de tiempo astronómicos, excluyendo la invención de alguna tecnología fantástica como los ordenadores cuánticos. La mayor parte del software de cifrado —incluso el escrito por expertos criptográficos extremadamente preocupados por la seguridad— no puede siquiera manejar claves más largas. Pero Avi insiste en usar Ordo, que por lo general se considera el mejor software de cifrado del mundo, porque puede manejar claves de longitud ilimitada... siempre que no te importe esperar a que calcule todos los números.

Randy empieza a teclear. No se molesta en mirar a la pantalla; mira por la ventana los focos de los *jeepneys* y los camiones. Está empleando una única mano, limitándose a golpear ligeramente en el teclado.

En el interior del ordenador de Randy hay un reloj preciso. Cuando pulsa una tecla, Ordo usa ese reloj para anotar el momento exacto, con precisión de microsegundos. Pulsa una tecla a las 03:05:56,935788 y otra a las 03:05:57,290664, ó 0,354876 segundos más tarde. Pulsa otra 0,372307 segundos más tarde.

Ordo registra todos esos intervalos y elimina los dígitos más significativos (en este ejemplo, el 0,35 y el 0,37) porque esas partes tenderán a ser similares en una pulsación y la siguiente.

Ordo quiere azar. Sólo quiere los dígitos menos significativos, digamos, el 76 y el 07 justo al final de los números. Quiere un buen montón de números al azar, y quiere que haya mucho, mucho azar. Está tomando números más o menos al azar y pasándolos por una función *hash* que añade todavía más azar. Ejecuta rutinas estadísticas sobre los resultados para asegurarse de que no contienen estructuras ocultas. Su ansia de azar es asombrosamente alta, y no dejará de pedirle a Randy que pulse el teclado hasta que no esté satisfecho.

Cuanto más larga es la clave que quieres generar, más largo es el proceso. Randy intenta generar una ridículamente larga. Le ha comentado a Avi, por medio de un mensaje cifrado, que si cada una de las partículas de materia del universo pudiese emplearse para construir un único superordenador cósmico, y ese ordenador trabajase en intentar romper la clave de cifrado de 4096 bits, le llevaría más tiempo que toda la vida estimada del universo.

— Empleando la tecnología actual —le respondió Avi — , eso es cierto. Pero ¿qué hay de los ordenadores cuánticos? ¿Y si se desarrollan nuevas técnicas matemáticas que simplifiquen la factorización de grandes números?

— ¿Cuánto tiempo quieres que sean secretos esos mensajes? —le preguntó Randy en el último mensaje antes de abandonar San Francisco—. ¿Cinco años? ¿Diez años? ¿Veinticinco años?

Después de llegar al hotel esa tarde, Randy descifró y leyó la respuesta de Avi. Todavía la tiene colgada frente a los ojos, como la imagen remanente de un *flash*.

Quiero que sigan siendo secretos mientras los hombres sean capaces del mal.

Sobre el *Criptonomicón*:
El *Criptonomicón* se ha convertido en una novela de culto de quienes se interesan en los temas de computación y criptografía. Su autor, Neal Stephenson, construye una novela en diferentes tiempos, los orígenes de los ordenadores durante la Segunda Guerra Mundial y la preocupación moderna por la criptografía.
En español se editó en tres volúmenes.

Los *hackers* y el desarrollo de la red

En realidad, los *hackers* han sido fundamentales en el desarrollo de Internet. Fueron *hackers* académicos quienes diseñaron los protocolos de Internet. Un *hacker*, **Ralph Tomlinson**, trabajador de la empresa BBN, inventó el correo electrónico en 1970, para uso de los primeros internautas, sin comercialización alguna. *Hackers* de los Bell Laboratories y de la Universidad de Berkeley desarrollaron UNIX. *Hackers* estudiantes inventaron el módem. Las redes de comunicación electrónica inventaron los tablones de anuncio, los chats, las listas electrónicas y todas las aplicaciones que hoy estructuran Internet. Y **Tim Berners-Lee** y **Roger Cailliau** diseñaron el *browser*/editor World Wide Web, por la pasión de programar, a escondidas de sus jefes en el CERN de Ginebra, en 1990, y lo difundieron en la red sin derechos de propiedad a partir de 1991. También el *browser* que popularizó el uso del World Wide Web, el Mosaic, fue diseñado en la Universidad de Illinois por otros dos *hackers* (**Marc Andreesen** y **Eric Bina**) en 1992. Y la tradición continúa: en estos momentos, dos tercios de los servidores de web utilizan Apache, un programa servidor diseñado y mantenido en *software* abierto y sin derechos de propiedad por una red cooperativa (Manuel Castells).

Ética del *hacker* y libertad del conocimiento

Los ***hackers***, en sentido estricto y tal como se lo entiende en el mundo de la computación, son, simplemente, personas con conocimientos técnicos informáticos cuya pasión es inventar programas y desarrollar formas nuevas de procesamiento de información y comunicación electrónica. Para ellos, un valor fundamental es la innovación tecnológica informática, para lo cual necesitan la posiblidad y libertad de acceso a los códigos fuente, libertad de acceso a la red, libertad de comunicación con otros *hackers*, espíritu de colaboración y de generosidad (poner a disposición de la comunidad de *hackers* todo lo que se sabe, y, en reciprocidad, recibir el mismo tratamiento de cualquier colega).

La actividad de algunos *hackers* se vincula con ideales políticos y luchan contra el control de los gobiernos y de las corporaciones sobre la red. Gran parte de su actividad se organiza en redes de colaboración en Internet.

Los *crackers*

Los ***crackers*** (del inglés *crack*, romper) son personas que a diferencia de los *hackers*, utilizan sus conocimientos para penetrar en redes, perturbar procesos, infundir alguna clase de daño o molestia, romper sistemas de seguridad y actividades de piratería. Los *crackers* no son bien considerados por la comunidad de *hackers*, puesto que usualmente se tiende a confundir a unos con otros.

Muchas veces los *crackers* son adolescentes que realizan sus actividades con el simple propósito de presumir o darse a conocer en la comunidad. Estas actividades pueden ser la difusión de virus, ingresar en redes... También existe una vertiente más política de los *crackers*, que utilizan la red para producir daño al enemigo, como se da entre *crackers* chechenios y rusos o entre *crackers* palestinos e israelíes.

Un interesante artículo sobre los hackers en http://www.ucm.es/info/dsip/clavel/talks/uned02/

Virus

¿Qué es un virus?

Se trata de un tipo de programa que, como los virus biológicos, es capaz de reproducirse autónomamente dentro de un sistema. Hay distintos tipos de virus, según el sector al que afecten: el sistema de arranque de la computadora, determinados archivos, partes de programas de uso frecuente, etc. Algunos son capaces de cambiar, o mutar, mientras están infectando un sistema. Al activarse, los virus pueden ejecutar diferentes acciones, desde colocar mensajes en la pantalla, bloquear aplicaciones o borrar archivos del disco duro.
Algunos virus no están diseñados específicamente para producir daño, sino sólo para dar a conocer su presencia. Esta clase de virus suele presentar mensajes textuales, auditivos o visuales. Se los conoce como "virus benignos".

Qué es un Caballo de Troya

Un archivo benigno en el que se imposta un código maligno es un Caballo de Troya o troyano. Se los conoce también como **impostores**. A diferencia de los virus, éstos no pueden replicarse a sí mismos. Al activarse el código dañino contenido dentro del archivo benigno, se provocan pérdidas o, incluso, robo de datos. Para que un Caballo de Troya se extienda, es necesario dejarlo entrar en el sistema, por ejemplo, abriendo un archivo adjunto de correo.

Representación del Caballo de Troya en una pieza de alfarería griega.

Actividad 9.3.

Presente griego

¿Por qué a este tipo de virus se lo llama Caballo de Troya?

¿Qué es un gusano?

Los gusanos son programas dañinos que pueden replicarse a sí mismos y transferirse entre sistema y sistema. A diferencia de los virus y los troyanos, no necesitan estar colocados dentro de otro archivo recipiente (el archivo infectado) para reproducirse. Sin embargo, muchos de los gusanos se encuentran dentro de archivos de Word o Excel, ya que pueden utilizar la función de "macros" de estos programas, que es la capacidad de programar y ejecutar instrucciones.

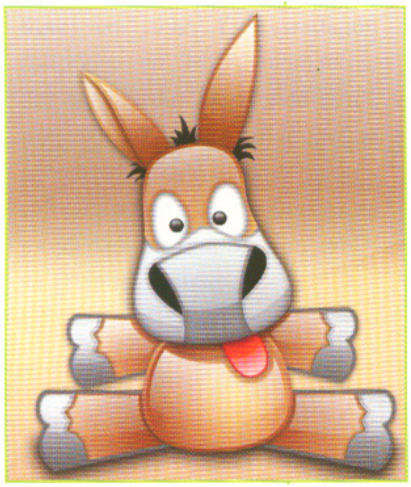
Los *hoax*

También existen programas que no son estrictamente virus, pero que pueden producir diversos tipos de daño. Son los denominados ***hoax*** (literalmente del inglés, "broma"), que no son verdaderos virus, pero que desde la masificación del correo electrónico, llegan a tener efectos parecidos. Los podemos detectar a menudo en los programas de correo, al recibir un mensaje que indica que se debe borrar algún archivo determinado porque es un virus, cuando en realidad se trata de un archivo importante para el sistema operativo. También en el caso de cadenas de mensajes falsas, en las que se pide ayuda para alguien enfermo, casos en los que, generalmente, se trata de recolectar direcciones válidas de correo electrónico para venderlas a quienes las usan con fines comerciales.

Para profundizar acerca de verdades y mitos sobre virus, *hoax* y otras alimañas, y, de paso, practicar inglés: http://vmyths.com/

Compartir archivos

Napster.



Emule.

Desde que la conexión a Internet se generalizó, comenzó a circular un nuevo modo de intercambio de información, programas, textos, música, etc. Lo que en los comienzos de Internet fue el intercambio académico, hoy en día cubre un amplio espectro.

Las redes de tipo ***peer to peer*** (ver **Capítulo 7**), al establecer una comunicación no basada en la relación cliente-servidor, sino en una donde cada nodo de la red puede actuar tanto como cliente y como servidor al mismo tiempo, permiten la implementación de programas que facilitan el intercambio de archivos.

La facilidad con la que se da este intercambio abre una controversia sobre la legalidad de esta práctica. Las grandes compañías discográficas iniciaron un juicio en 1999 contra el primero de estos sistemas, **Napster**, lo que obligó al cierre de este servicio.

En la actualidad, la evolución de las conexiones de banda ancha permite no sólo el intercambio de canciones en formato mp3, sino también de álbumes completos y películas en formato DiVX, a través del cual se comprime una película en calidad de imagen de DVD, de manera que quepa en un CD.

El debate está abierto y las compañías discográficas y algunos estudios cinematográficos han logrado autorización judicial para que

los proveedores de Internet faciliten la información sobre qué usuarios han hecho intercambios de archivos de material protegido por *copyright*, para iniciar demandas judiciales.
Lamentablemente estos programas son conocidos como un recurso para acceder al *software* de manera ilegal, pero no es esto lo único que se puede hallar en este pequeño "universo".

Derechos y propiedad: ¿Cuál es la cuestión?

Una persona entra a un negocio y compra un cd de música. ¿A quién le pertenece el objeto comprado? No cabe duda de que el objeto en sí, los átomos que conforman el cd, son propiedad de quien lo compró. Puede poseerlo, tirarlo, usarlo como posavasos o como adorno en el espejo retrovisor del coche. Sin embargo, la posesión física del objeto cd, no es lo mismo que la posesión de los *bytes* y de la información contenidos en él. ¿A quién le pertenece la música grabada? Al comprar el cd, si bien se compra el objeto, sólo se adquieren los derechos de "hacer un uso justo" de la música contenida en él. Por ese motivo, no está permitido hacer copias de los cd, y muchas compañías ponen trabas al intercambio de archivos por Internet.

Los Estados Nacionales y la utilización del *software* libre

Desde hace unos años viene avanzando la idea del uso de *software* libre por parte de los Estados Nacionales. No siempre se comprende bien la idea central de estas declaraciones. Pues es erróneo suponer que el foco está puesto sobre el aspecto de la gratuidad. Por otra parte, *software* libre no es sinónimo de *software* gratuito. De hecho existen todas las combinaciones posibles. El navegador Internet Explorer es gratuito y propietario. Algunas distribuciones de GNU/Linux como SuSE son libres y costosas. Así como existe *software* libre y gratuito, como el OpenOffice, y, por supuesto, el *software* costoso y propietario como la suite Office de Microsoft.
La importancia radica en que el *software* libre de código abierto permite que un especialista examine el código fuente.

El caso del Perú

Cuando se presentó en el congreso de la República del Perú el proyecto sobre la utilización del *software* libre (Proyecto de Ley N° 1609, *Software* Libre en la Administración Pública), se planteó una controversia con los principales productores de *software* pro-

Software libre. Para ampliar:

Venezuela:
http://www.rnv.gov.ve/noticias/?act=ST&f=2&t=89
30 de octubre de 2004.

Perú:
http://www.opensource.org/docs/peru_to_ms_spanish.php
de abril de 2002.

pietario. Pero los argumentos fueron esencialmente que la utilización por parte del Estado tiene las siguientes características:

"Los principios elementales que animan al Proyecto se vinculan a las garantías básicas de un Estado democrático de derecho, como:

- Libre acceso del ciudadano a la información pública.
- Perennidad de los datos públicos.
- Seguridad del Estado y de los ciudadanos.

Para garantizar el libre acceso de los ciudadanos a la información pública, resulta indispensable que la codificación de los datos no esté ligada a un único proveedor. El uso de formatos estándar y abiertos permite garantizar este libre acceso, logrando si fuera necesario la creación de *software* libre compatible.
Para garantizar la perennidad de los datos públicos, es indispensable que la utilización y el mantenimiento del *software* no dependan de la buena voluntad de los proveedores, ni de las condiciones monopólicas impuestas por éstos. Por ello el Estado necesita sistemas cuya evolución pueda ser garantizada gracias a la disponibilidad del código fuente.
Para garantizar la seguridad del Estado o seguridad nacional, resulta indispensable contar con sistemas desprovistos de elementos que permitan el control a distancia o la transmisión no deseada de información a terceros. Por lo tanto, se requieren sistemas cuyo código fuente sea libremente accesible al público para permitir su examen por el propio Estado, los ciudadanos y un gran número de expertos independientes en el mundo. Nuestra propuesta aporta mayor seguridad, pues el conocimiento del código fuente eliminará el creciente número de programas con *código espía*."

Edgar David Villanueva Núñez,
congresista de la República del Perú. Texto extraído de
http://www.opensource.org/docs/peru_to_ms_spanish.php

Actividad 9.4.

¿Libre o propietario?

Averigüen qué organismos estatales de la zona trabajan con *software* libre. Busquen en Internet si existe reglamentación sobre este tema.

Independencia informática nacional
Gobierno decretará uso del *software* libre para la administración pública

El presidente de la República, Hugo Chávez Frías, anunció que el Gobierno emitirá un decreto mediante el cual se establecerá la utilización de *software* libre para todas los organismos y dependencias de la administración pública.

...

La intención de esta medida es lograr independencia tecnológica e informática, "ya el Brasil lo ha anunciado y Venezuela va por el mismo camino".

La ministra de Ciencia y Tecnología, Yadira Córdoba, refirió que "todos los Infocentros están trabajando con *software* libre, el proyecto Alcaldía Digital, al que se han incorporado 81 municipios, también se montó sobre *software* libre y toda la plataforma del Ministerio de Ciencia y Tecnología (MCT) está hecho sobre *software* libre".

El MCT ha venido capacitando a sus funcionarios y haciendo seminarios, de carácter nacional e internacional, para abrir caminos hacia lo que es el *software* libre.

No hemos querido que esto se imponga abruptamente porque significaría hacer un cambio de cultura y de visión; por el contrario, queremos ir incorporando el *software* libre progresivamente y creo que con el trabajo que hemos venido realizando en el último año, hay condiciones suficientes para dar este paso, dijo la ministra Yadira Córdoba.

El presidente Chávez insistió que la decisión obedece a "la independencia científica nacional, para no seguir dependiendo del *software* de propietarios, si el conocimiento no tiene propietarios, la propiedad intelectual es una trampa del neoliberalismo".

Del sitio de la Radio Nacional
de Venezuela
http://www.rnv.gov.ve/noticias/
?act=ST&f=2&t=8930

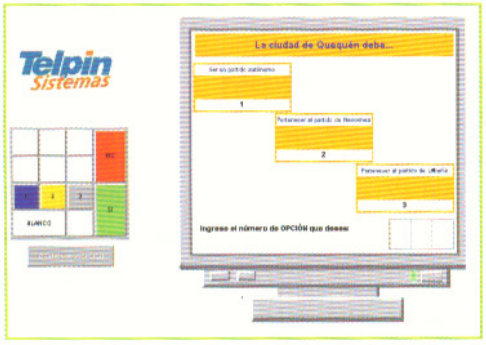
¿Desde cuándo se votará de manera electrónica?

El tema del voto electrónico ha estado circulando durante los últimos años, sobre todo, luego de los sospechados comicios en países latinoamericanos y en las elecciones de los Estados Unidos en el año 2000.

El voto electrónico se refiere a la instalación de casillas de votación similares a cajeros automáticos de los bancos, en las cuales el votante ingresará directamente su voto, evitando de esta manera la intervención humana y por tanto toda posibilidad de manipulación de los resultados.

La preservación y el ejercicio de la democracia se convierten en áreas donde las Tics podrían aportar su potencial, de allí el entusiasmo de quienes proponen la implementación de estos sistemas. Sin embargo, esta idea plantea varios interrogantes. Se enunciarán algunos de ellos:

Las casillas de votación utilizarán algún *software*. ¿De código abierto o propietario? ¿Cómo se garantiza la "pureza del programa" y que no tenga cláusulas ocultas que modifiquen los resultados? ¿Puede quedar el manejo de los datos sobre elecciones en manos privadas? ¿Cómo se garantiza la seguridad y la imposibilidad de intervenciones electrónicas en el sistema? ¿Qué clase de respaldo existe en el caso de que surjan dudas sobre los resultados obtenidos de manera electrónica y esos resultados deban ser contrastados?



Hace falta ajustar algunas variables para que los beneficios del voto electrónico sean mayores que los del voto en papeles, aunque es innegable que más tarde o más temprano resulta un modo mucho más razonable, desde el punto de vista administrativo.

Hay un proyecto para reemplazar los documentos nacionales de identidad asociado al voto electrónico para que no sea necesario un registro de sello en un documento de papel. Además permitiría confeccionar un documento mucho más seguro que en la actualidad.

Ver nota en el sitio del diario Clarín del 12/06/2004
http://old.clarin.com/diario/2004/12/06/elpais/p-00501.htm

Actividad 9.5.

Cliqueá y votá

Busquen información sobre este tema en notas periodísticas de actualidad. Investiguen en qué otros países hay voto electrónico. ¿Saben si en nuestro país se hizo alguna experiencia? ¿Qué debería tenerse en cuenta previamente para impulsar esta modalidad?

Un paso más allá. El futuro que está por llegar

¿Podrán pensar las máquinas? Inteligencia artificial

La **inteligencia artificial** es un campo de investigación y aplicación que trata de conseguir que las computadoras simulen en cierta manera la inteligencia humana. El problema es que la inteligencia humana es difícil de circunscribir y definir. En efecto, la inteligencia es una conducta compleja que incluye la conciencia, el inconsciente, los procesos cognoscitivos.

Existen dos líneas de investigación sobre inteligencia artificial: **inteligencia artificial dura** e **inteligencia artificial blanda**.

Inteligencia artificial dura

La inteligencia artificial dura se propone la creación de formas de inteligencia basada en las computadoras, que pueda razonar y resolver problemas. En teoría, esta forma de inteligencia artificial debería ser consciente de sí misma.

Un ejemplo de este tipo de inteligencia artificial, es el computador **HAL 9000** de la película *2001 Odisea del Espacio*, mencionada en el **Capítulo 2.**

Existen a su vez **dos variantes de inteligencia artificial dura**: una en la que se imita la forma de pensar y razonar de los humanos, y otra en la que se propone una manera no humana de pensar y razonar.

¿Inteligencia artificial dura o blanda?

Inteligencia artificial blanda

En este caso, el objetivo es la creación de una inteligencia basada en máquinas, que sólo pueda ser operacional dentro de un dominio limitado. No se pretenden máquinas inteligentes e independientes, sino adecuadas solamente para una tarea específica. Uno de los ejemplos más ilustrativos se da cuando se hace referencia a los *edificios inteligentes*, que son aquellos que poseen dispositivos para regular la temperatura de los ambientes, cerrar puertas y ventanas, registrar la entrada o salida de personas, encender electrodomésticos, etcétera.

El campo de desarrollo de la inteligencia artificial es muy discutido y debatido desde diversas perspectivas, desde lo filosófico hasta lo psicológico. Hasta el momento se han logrado muy pocos avances. Derivados de la investigación sobre inteligencia artificial, existen en la actualidad algunos dispositivos:

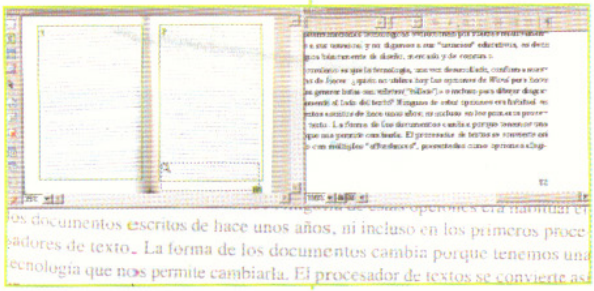
Chinook: *software* para jugar a las damas, triunfador en el Campeonato Mundial de Hombre y Máquinas de 1994.
Más información, en http://www.cs.ualberta.ca/~chinook

Escena de la partida entre Kasparov y Deep Blue.

Deep Blue: supercomputadora producida por IBM, para jugar al ajedrez, que venció a Garry Kasparov en 1997.

Fuzzy logic: técnica para razonar bajo condiciones de falta de certeza. Es utilizada en sistemas de control industrial.

***Softwares* para traducción de idiomas**: su empleo es cada vez más difundido, aunque los resultados son muy pobres comparados con las traducciones realizadas por personas.



Pantalla de un programa de OCr que a partir de una imagen de un texto "lee y reconoce" las letras para convertirlo en un archivo de texto.

Reconocimiento óptico de datos: (OCR: *Optical character recognition*): aplicaciones que pueden leer un archivo de imagen que contiene texto, obtenido por un escáner, y convertirlo en un archivo de texto para ser modificado por un procesador de palabras.

Reconocimiento de escritura: aplicación similar a la anterior, que reconoce texto a partir de la lectura de letra manuscrita. Muy utilizado en los asistentes digitales personales.

Reconocimiento de voz: es la capacidad de una máquina de responder a estímulos sonoros. Existen versiones comerciales y son de gran utilidad para el manejo de la computadora para personas con discapacidad.

Visión artificial: la lectura y comprensión de imágenes de manera automática se utiliza en procesos industriales y de seguridad.

Realidad virtual

La **realidad virtual** invita a soñar con poder vivir eventos sin los riesgos que conlleva la realidad. El planteo y los avances en este terreno, muy desarrollado en los video juegos para el gran pú-

blico, hacen imaginar las más diversas excursiones, rompiendo incluso las barreras del tiempo y del espacio. Pero esto no es todo. Hay que partir de la definición más elemental.

¿Qué es Realidad virtual?

"Definitivamente un término muy sonado y controversial. En estos días en que todo es virtual, existe mucha confusión en las personas expuestas de una u otra forma a los nuevos medios. En el nombre en sí ya hay una gran contradicción: Realidad Virtual. Algo que es, pero no es. La **realidad virtual** es una representación de las cosas a través de medios electrónicos, que **da la sensación de estar en una situación real en la que podemos interactuar con lo que nos rodea**.

La realidad virtual puede ser de dos tipos: **inmersiva** y **no inmersiva**. Los métodos inmersivos de realidad virtual con frecuencia se ligan a un ambiente tridimensional creado por computadora, el cual se manipula a través de cascos, guantes u otros dispositivos que capturan la posición y rotación de diferentes partes del cuerpo humano. La realidad virtual no inmersiva utiliza medios como el que actualmente nos ofrece Internet, en el cual se puede interactuar a tiempo real con diferentes personas en espacios y ambientes que en realidad no existen, sin la necesidad de dispositivos adicionales a la computadora.

Sin llegar a los extremos propios de la ciencia ficción y para los cuales los presupuestos se elevarían de un modo inconmensurable, es posible vislumbrar aplicaciones más pedestres que mejoren la vida cotidiana y conviertan a las máquinas en excelentes auxiliares en la resolución de problemas complejos. Tanto en los terrenos del aprendizaje y la enseñanza, el entrenamiento para funciones técnicas como los pilotos de aviones, solucionar problemas médicos o modelar lugares inaccesibles al humano, son aplicaciones que ya encuentran diversos grados de avance. Seguramente es cuestión de tiempo para llegar a una más completa conexión y para experimentar más sensaciones propias de los entornos virtuales en la medida en que se puedan ir precisando las interfaces de usuario, pero es fundamental destacar lo que ya se puede hacer hoy".

Tomado de: http://www.activamente.com.mx/vrml/

Un guante sirve para interactuar con la realidad virtual.

Persona utilizando interfaces.

¿Triste y solitario final para los libros?

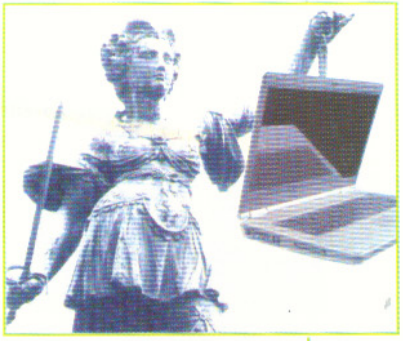
Myfriend, un *hardware* para la lectura de libros electrónicos (*e-books*).

El desarrollo y potencial de la escritura hipertextual ha llevado a muchos autores a proclamar que la muerte de los libros está próxima. El tema, sin embargo, posee muchas aristas que deben ser analizadas cuidadosamente para comprender las propiedades, particularidades, ventajas y deficiencias de cada uno de estos sistemas de escritura y de transmisión.

Derrick de Kerckhove sostiene que a diferencia de la red y la pantalla, donde las palabras "corren", el libro es un lugar de reposo de las letras, lo que permite una reflexión más profunda sobre lo que se está leyendo. Señala el autor que, en el momento de la aparición de los libros, éstos favorecieron la difusión de la cultura. En la actualidad, este efecto de ralentización de los libros, sirve para llamar a la reflexión en el contexto de la vorágine informativa.

Sin embargo los libros aún tienen una ventaja más sobre todas las otras tecnologías: su interfaz de usuario. Son fácilmente transportables y se pueden leer en cualquier lado, sin necesidad de conexiones, electricidad, ni implementos auxiliares.

¿Pueden las máquinas tomar decisiones?



Ni tu papá ni tu mamá, ¿será la máquina quien decida? Presioná F4 para saber si podés salir este sábado a bailar.

La posibilidad de las máquinas de tomar decisiones puede ser abordada a partir del siguiente ejemplo:

Un coche es equipado con un sistema que evalúa el nivel de alcohol en la sangre del conductor, y cuando el nivel supera la norma establecida, impide que el coche se ponga en marcha para evitar accidentes. En un determinado caso, una persona sufre un ataque y debe ser conducido con urgencia al hospital para salvar su vida. Se encuentran en un lugar alejado sin posibilidad de contacto telefónico para pedir auxilio. La única persona que puede conducir ha bebido de más, por lo que el dispositivo impide que el coche se ponga en marcha y la persona fallece.

A través de este ejemplo, puede observarse el problema que plantea dejar en manos de las computadoras la toma de decisiones, ya que éstas siguen las instrucciones con las cuales fueron programadas para tomar la decisión, sin tener en cuenta posibles casos excepcionales como el descripto.

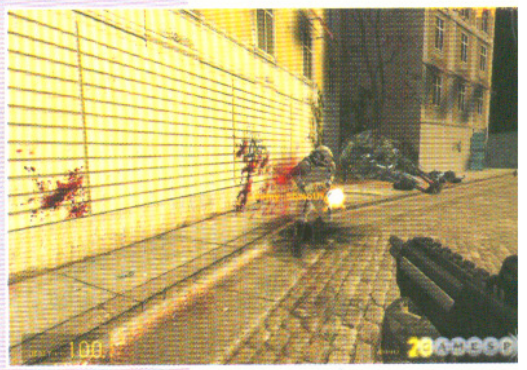
Como contraargumento, suele opinarse que las máquinas, de hecho, no toman decisiones, ya que las decisiones fueron tomadas de antemano en el momento de programar la máquina y considerar cada una de las variantes. El problema, de naturaleza ética, surge cuando una máquina, sea decidiendo o aplicando una decisión tomada previamente cuando se la programó, evita que un humano realice una acción.

Violencia y videojuegos

¿Los video juegos nos convierten en personas agresivas y son culpables de la escalada de violencia en la sociedad?
El siguiente artículo presenta diversas posiciones respecto al tema de los video juegos:

Juegos violentos
Francis Pisan, Silicon Valley.

Una de las grandes ferias de juegos electrónicos acaba de reunirse en Atlanta (Capital del Estado de Georgia, EE.UU.). Una excelente ocasión para ver lo último en materia de juegos. Varios observadores han notado un cierto esfuerzo de los fabricantes por atraer públicos nuevos, niñas o personas maduras, y sacar así la preponderancia de los juegos para machos adolescentes, fácilmente atraídos por la violencia.
Pero muy a pesar de los organizares, E3 (Electronic Enternaiment Expo), la feria, tuvo lugar poco días después de una matanza perpetrada por un adolescente en una escuela del Estado de Oregon, y no tan lejos de la que tuvo lugar en Jonesboro, Estado de Arkansas, durante el mes de abril. En total son cuatro los dramas de este tipo en los últimos meses.
Doug Lowenstein, presidente de la Asociación de Soportes Lógicos Interactivos, declaró de manera categórica que "los videojuegos no son la fuente de violencia en nuestra sociedad", y recalcó que, según un estudio reciente el 40% de los consumidores estiman que son la forma más excitante de pasar el tiempo en casa, más que ver la televisión, leer libros o navegar por Internet. "Los juegos no tienen la culpa", dijo Lowenstein, "sería como achacarle el analfabetismo a la televisión. Es hora de que tomemos en cuenta el acceso libre a las armas y a las familias disfuncionales". Los juegos pueden no ser la causa de la violencia en EE.UU. El problema es determinar en qué medida contribuyen a ella, con el



acceso fácil a las armas, las familias con problemas y los centenares de asesinatos que se pueden ver cada día por la televisión. El artículo que relata la conferencia de prensa de Lowenstein para la reviste en línea ZDnet, abre una interesante discusión en la que participan una mayoría de ingenieros, para quienes los juegos no tienen nada que ver. Pero existen matices.

Un participante se sorprende con amarga ironía de ver que quienes niegan la influencia de los juegos violentos sobre la gente insisten sobre su gran éxito. Los compramos por algo, dice, y añade: No sugiero que los prohibamos, pero no seamos ingenuos".

Un adolescente de 15 años afirma que "ciertos niños son malos, nacieron sin conocimiento del bien y del mal. A mis amigos y a mí nos gusta mucho jugar al quake2 por Internet, mutilar y destripar a otra gente. ¿Pero querrá decir esto que me va a influir para que lleve un cuchillo a la escuela y haga daño a otro? Tal vez, si no fuera mentalmente estable".

"Los niños siempre han tenido impulsos violentos", dice otro comentario, "el problema es que en ninguna parte, excepto en Estados Unidos, tienen acceso a los medios que pueden provocar una muerte real.

El País, 2 de junio de 1998.

Actividad 9.6.

Juicio a los video juegos

Les proponemos un debate: Divídanse en dos grupos, uno a favor del uso de los video juegos y otro que argumente en contra de éstos. Pueden fundamentar sus posturas a partir del artículo leído, así como también pueden buscar argumentos en otras fuentes.

Actividad 9.7.

Cada cual atiende su juego...

a) Realicen una encuesta sobre las preferencias de los video juegos. Investiguen cuáles son los preferidos según las edades y el sexo. Dónde los juegan y cuántas horas semanales les dedican. Elaboren una nota de opinión a partir de las conclusiones obtenidas.

b) Realicen una lista de sus video juegos preferidos. Clasifíquenlos por tipo: de simulación, estrategia, juegos de rol, etc. Por objetivo o misión. Por el contexto en el que se desarrollan, etc.

Reflexiones finales

En el contexto de la alfabetización digital y de la formación de ciudadanos-usuarios críticos, es importante estar al tanto de lo que significan los nuevos modos de intercambio y las reglas que se están estableciendo.

Es importante tener presente que el valor de los avances de la humanidad debe redundar en beneficio de la convivencia y del progreso. No del control creciente y de la incomunicación y la soledad.

A lo largo de este libro se ha planteado tanto el conocer los avances tecnológicos, como así también su imbricación y consecuencias en el tejido social.

El desarrollo y expansión de la tecnología de red, y la creación del ciberespacio como un espacio de interacción, abren la posibilidad y el reto en la construcción de un futuro más justo. Internet tiene lo bueno y lo malo del mundo, no se le pueden atribuir los problemas del terrorismo, ni del abuso, ni la violencia social, que ya existían antes. Aún hoy se responsabiliza a la televisión de inspirar y hasta causar la violencia y la delincuencia.

Tampoco cabe esperar que la sola presencia de las tecnologías solucione los problemas de hambre, falta de educación y desigualdad de acceso a bienes materiales y culturales. Es que en ambos casos, los aportes tecnológicos son más o menos laterales a la resolución de cuestiones sociales.

En todo caso, la discusión debería centrarse en qué uso se puede hacer de los crecientes recursos materiales y tecnológicos y, fundamentalmente, cómo se distribuyen. Este no es un problema nuevo, pero vale la pena plantearlo otra vez ante nuevos horizontes del progreso humano.

Si buena parte de lo que los seres humanos estamos entendiendo y pudiendo materializar es volcado hacia una mejor convivencia y comunicación, será posible que nuevas generaciones reconozcan nuevos valores. En ese caso, las preocupaciones podrán desplazarse desde cómo generar modos más eficaces de destruir al diferente, para imaginar maneras mejores de potenciar las semillas diseminadas por doquier, integrando los aportes para vivir mejor.

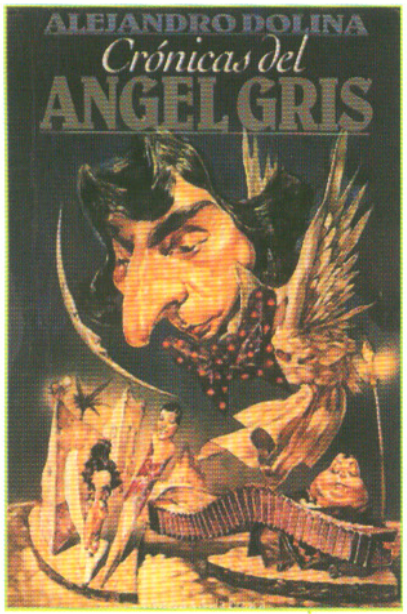
La utopía de la colaboración mutua y del crecimiento conjunto y solidario siguen siendo una meta para quienes impulsan la apertura y la honestidad. La cultura y la ciencia han progresado fundamentalmente por la generosidad de quienes pusieron sus conocimientos al servicio de la humanidad.

"El objetivo de la ciencia no es abrir las puertas de la infinita sabiduría, sino poner un límite al infinito error" **Bertolt Brecht** en *Vida de Galilei.*

El lugar del progreso científico-técnico

"...Yo considero que el único fin de la ciencia consiste en aliviar la miseria de la existencia humana. Si los hombres de ciencia, amedrentados por los déspotas, se conforman con acumular conocimientos por el conocimiento mismo, la ciencia puede convertirse en un inválido, y las nuevas máquinas sólo significarán nuevas calamidades."

Bertolt Brecht



Portada del libro *Crónicas del Ángel Gris*. Edición publicada por Ediciones de la Urraca.

Es interesante compartir el punto de vista de Alejandro Dolina que propone una forma de entender la potencia de los vínculos humanos en sus

Instrucciones para elegir en un picado

Cuando un grupo de amigos no enrolados en ningún equipo se dispone para jugar, tiene lugar una emocionante ceremonia destinada a establecer quiénes integrarán los dos bandos. Generalmente dos jugadores se enfrentan en un sorteo o pisada y luego cada uno de ellos elige alternativamente a sus futuros compañeros.

Se supone que los más diestros son elegidos en los primeros turnos, quedando para el final los troncos. Pocos han reparado en el contenido dramático de estos lances.

El hombre que está esperando ser elegido vive una situación que rara vez se da en la vida. Sabrá de un modo brutal y exacto en qué medida lo aceptan o lo rechazan. Sin eufemismos, conocerá su verdadera posición en el grupo. A lo largo de los años, muchos futbolistas advertirán su decadencia, conforme su elección sea cada vez más demorada.

Manuel Mandeb, que casi siempre oficiaba de elector, observó que las decisiones no siempre recaían sobre los más hábiles. En un principio se creyó poseedor de vaya a saber qué sutilezas de orden técnico, que le hacían preferir compañeros que reunían ciertas cualidades.

Pero un día comprendió que lo que en verdad deseaba, era jugar con sus amigos más queridos. Por eso elegía a los que estaban más cerca de su corazón, aunque no fueran tan capaces.

El criterio de Mandeb parece apenas sentimental, pero es también estratégico. Uno juega mejor con sus amigos. Ellos serán generosos, lo ayudarán, lo comprenderán, lo alentarán y lo perdonarán. Un equipo de hombres que se respetan y se quieren es invencible. Y si no lo es, más vale compartir la derrota con amigos, que la victoria con los extraños o los indeseables.

Dolina, Alejandro: *Crónicas del Ángel Gris*, 1988. Actualmente en Ediciones Colihue, Buenos Aires.