SEGURIDAD INFORMATICA

Introducción

1. **Seguridad Informática**
2. **Mecanismos de seguridad**
3. **Contraseñas**
4. **Firewalls**
5. **Encriptación**
6. **Antivirus**
7. **Contraseñas: se roban cada vez más**
8. **Recomendaciones**
9. **La tiranía de la era digital amenaza el espíritu crítico**
10. **Conclusiones – Ponencia**

Autor: ***Esc. Ana María KEMPER – ARGENTINA***

INTRODUCCION

Los expertos en el tema, y, quienes han estudiado informática y sistemas han definido a la seguridad informática como: *el conjunto de procedimiento, y herramientas informáticas, cuyo objetivo es garantizar la disponibilidad, integridad, confidencialidad, autenticidad y buen uso de la información que reside en un sistema de información y sus bases de datos.*

Cada día máspersonas mal intencionadas intentan tener acceso a los datos de nuestras computadoras y ocasionar en la gran mayoría de los casos graves problemas .
Uno de las posibles consecuencias de una intrusión es la **pérdida de datos**. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día con las copias de seguridad. (back up) Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.
Otro de los problemas más dañinos es el **robo de información** sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes, lo que puede acarrear demandas millonarias contra esta, o un ejemplo más cercano es el robo de nuestras contraseñas, de todas o cualquiera de las cuentas de correo por las que intercambiamos información con otros.

Con la constante evolución de las computadoras, es fundamental saber que recursos se necesitan para obtener seguridad en los sistemas de información.

El presente trabajo y mi ponencia tienen como objetivo comprender los conceptos básicos de seguridad informática

- Conocer los factores de riegos
- Conocer los mecanismos de seguridad informática
- Describir los principales problemas de seguridad informática con los que se enfrentas los usuarios de computadoras.
- Conocer los conceptos de integridad, confiabilidad, y autenticidad existente.
- Concientizar sobre los riesgos a los que las organizaciones y usuarios de computadoras se enfrentan en materia de seguridad de la información
- Y por último ampliar o enriquecer los conocimientos acerca de la seguridad informática

Como definimos en un principio, la seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

Ello con un objetivo y fin:que los recursos del sistema de información (material informático o programas) sean utilizados de la manera que se decidió en su programación, y que, el acceso a la información allí contenida, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

En nuestra actividad de Notarios, debemos contar con que la información que obtenemos por medios informáticos sea confiable, autentica y segura, lo cual, al no haber sido íntegramente logrado, se obtiene en la mayoría de los casos, como simple "información".-

Tal es el caso del Registro de la Propiedad o Mercantil, que han puesto a disposición de los usuarios, en algunos casos con registro previo, en otros con el numero de trámite, y/o algún otro requisito que se halla definido en el acceso a esta información.- En la mayoría de los casos, la información y datos que se obtienen. son auténticos y certeros, pero a la hora de darles validez legal, necesitamos la información vertida en soporte papel.-

PRINCIPIOS de SEGURIDAD INFORMATICA

Para lograr sus objetivos la seguridad informática se fundamenta en principios, que debe cumplir todo sistema informático:

Confidencialidad: Consiste en hacer que la información sea ininteligible para aquellos individuos que no estén involucrados en la operación. Basándose en este principio, las herramientas de seguridad informática deben proteger el sistema de invasiones y accesos por parte de personas o programas no autorizados. Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que los usuarios, computadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

Integridad: La integridad consiste en hacer que la información que se obtenga, no se hayaalterado durante la transmisión (accidental o intencionalmente).

Autenticación: Asegurar que sólo las personas autorizadas y registradas tengan acceso a los datos, es decir la confirmación de la identidad informada por el usuario; la garantía para cada una de las partes de que su interlocutor es realmente quien dice ser. Un control de acceso permite (por ejemplo gracias a una contraseña codificada) garantizar el acceso a recursos únicamente a las personas autorizadas.
Asimismo se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén bien sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos. Este principio es importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, computadores y procesos comparten la misma información.

Disponibilidad: El principio de la disponibilidad es garantizar el acceso a un servicio o a los recursos, previo cumplimiento de los requisitos para ello, con la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático. Basándose en este principio, las herramientas de seguridad informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia que requieran.- Este principio es importante en sistemas informáticos cuyos compromiso con el usuario, es prestar servicio permanente.

No repudio: Constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada. Garantizar que no puedan negar una operación realizada.

En nuestra actividad notarial, los datos que informamos a nuestros colegios, los informes que logramos de los sitios web de los Registros de la Propiedad, del Registro Público de Comercio, del Registro Civil, del Registro de Actos de Ultima Voluntad, son datos que sola mente pueden ser utilizados por notarios (usuarios) registrados

previamente, y por ahora, son simplemente informativos, con la excepción del Registro de Actos de Ultima Voluntad que tiene un avance mayor en su desarrollo telemático.

FACTORES DE RIESGO

Ambientales/Físicos: factores externos, lluvias, inundaciones, terremotos, tormentas, rayos, humedad, calor entre otros.

Tecnológicos: Fallas de hardware y/o software, fallas en el aire acondicionado, falla en el servicio eléctrico, ataque por virus informático, etc.

Humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, alteraciones etc.

La seguridad de los sistemas de información es objeto de metáforas, ya que más de una a vez se la compara con una cadena, afirmándose que el nivel de seguridad de un sistema es efectivo únicamente si el nivel de seguridad del eslabón más débil también lo es. De la misma forma, una puerta blindada no sirve para proteger un edificio si se dejan las ventanas completamente abiertas.

Lo que se trata de demostrar es que se debe afrontar el tema de la seguridad a nivel global y que debe constar de los siguientes elementos:

- Concientizar a los usuarios acerca de los problemas de seguridad
- Seguridad lógica, es decir, la seguridad a nivel de los datos, en especial los datos almacenados, sus aplicaciones e incluso los sistemas operativos de cada uno de ellos.-.
- Seguridad en las telecomunicaciones: tecnologías de red, servidores de compañías, redes de acceso, etc.
- Seguridad física, o la seguridad de infraestructuras materiales: asegurar las habitaciones, los lugares abiertos al público, las áreas comunes de la Notaria, las estaciones de trabajo de los empleados, etc.

MECANISMOS DE SEGURIDAD

Un mecanismo de seguridad informática es una técnica o herramienta que se utiliza para fortalecer la confidencialidad, la integridad y/o la disponibilidad de un sistema informático.

Existen muchos y variados mecanismos de seguridad informática. Su selección depende del tipo de sistema, de su función y de los factores de riesgo que lo amenazan.

Clasificación según su función:

Preventivos: Actúan antes de que un hecho ocurra y su función es detener agentes no deseados.
Detectivos: Actúan antes de que un hecho ocurra y su función es revelar la presencia de agentes no deseados en algún componente del sistema. Se caracterizan por enviar un aviso y registrar la incidencia.
Correctivos: Actúan luego de ocurrido el hecho y su función es corregir la consecuencias.

Según un informe del CongressionalResearchService, las computadoras tienen dos características inherentes que las dejan abiertas a ataques o errores operativos:

1.-Una computadora hace exactamente lo que está programada para hacer, incluyendo la revelación de información importante. Un sistema puede ser reprogramado por cualquier persona que tenga los conocimientos adecuados.

2.-Cualquier computadora puede hacer sólo aquello para lo que está programada, no puede protegerse a sí misma contra un mal funcionamiento o un ataque deliberado a menos que este tipo de eventos haya sido previsto de antemano y se hayan puesto medidas necesarias para evitarlos.

Los propietarios de computadoras y los administradores utilizan una gran variedad de técnicas de seguridad para protegerse:

Restricciones al acceso Físico: Esta consiste en la aplicación de barreras y procedimientos de control , como medidas de prevención y contramedidas ante amenazas a los recursos de información confidencial.

Por ej: El Ratón U-Match Bio-Link, comprueba la huella del pulgar del usuario. Contra una base de datos que contiene las huellas autorizadas.

Debe haber controles y mecanismos de seguridad dentro y alrededor del computador, server o hardware que exista en determinado medio, y la estricta restricción a los medios de accesos remoto al y desde el mismo, implementados para proteger el hardware y medios de almacenamiento de datos.

Una forma de reducir las brechas de seguridad es asegurarse de que sólo las personas autorizadas pueden acceder a una determinada máquina.

Las organizaciones utilizan una gran variedad deherramientas técnicas para identificar a su personal autorizado. Las computadoras pueden llevar a cabo ciertas comprobaciones de seguridad, los guardias de seguridad humanos otras. En función del sistema de seguridad implementado, podrá acceder a un sistema en función a:

Algo que usted tenga: Una llave, una tarjeta de identificación con una fotografía o una tarjeta inteligente que contenga una identificación digital codificada almacenada en un chip de memoria.

Algo que usted conozca: una contraseña, un número de identificación, una combinación de bloqueo o algo de su historial personal.

Algo que usted haga: Su firma o su velocidad de escritura y los patrones de error.

Algo suyo: (Sistema Biométrico) La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas., La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona **por lo que es** (manos, ojos, huellas digitales y voz).

Los Beneficios de una Tecnología Biométrica pueden eliminar la necesidad de poseer una tarjeta para acceder.

Huella Digital Basado en el principio de que no existen dos huellas dactilares iguales, este sistema viene siendo utilizado desde el siglo pasado con excelentes resultados. Cada huella digital posee pequeños arcos, ángulos, bucles, remolinos, etc. (llamados minucias) características y la posición relativa de cada una de ellas es lo analizado para establecer la identificación de una persona. Esta aceptado que dos personas no tienen más de ocho minucias iguales y cada una posee más de 30, lo que hace al método sumamente confiable.

Verificación de Voz: La dicción de una (o más) frase es grabada y en el acceso se compara la vos (entonación, diptongos, agudeza, etc.). Este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.

Verificación de Patrones Oculares: Estos modelos pueden estar basados en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0).

CONTRASEÑAS

Las contraseñas son las herramientas más utilizadas para restringir el acceso a los sistemas informáticos. Sin embargo, sólo son efectivas si se escogen con cuidado, la mayor parte de los usuarios de computadoras escogen contraseñas que son fáciles de adivinar: El nombre de la pareja, el de un hijo o el de una mascota, palabras relacionadas con trabajos o aficiones o caracteres consecutivos del teclado. Un estudio descubrió que las contraseñas favoritas en el Reino Unido son Fred-God, mientras que en América eran, Love- sexy, . Los hackers conocen y explotan estos clichés, por lo que un usuario precavido no debe utilizarlos. Muchos sistemas de seguridad no permiten que los usuarios utilicen palabras reales o nombres como contraseñas, evitando así que los hackers puedan usar diccionarios para adivinarlas. Incluso la mejor contraseña sebe cambiarse periódicamente.

Combine letras, números y símbolos. Cuanto más diversos sean los tipos de caracteres de la contraseña, más difícil será adivinarla.

En sistemas informáticos, mantener una buena política de seguridad de creación, mantenimiento y recambio de claves es un punto crítico para resguardar la seguridad y

privacidad. Por ello, normalmente, los bancos obligan a los usuarios al cambio de contraseña, luego de un periodo de haber sido utilizada, por una nueva, totalmente distinta, y que servirá por otro periodo determinado. Las oficinas publicas NO exigen a los Notarios estos cambios, ya que, todas las veces que accedemos es para informar datos de nuestra actividad, y esa contraseña, no tiene registros de haber sido adulterada, violada o interceptada.

Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos (incluso con varias computadoras a la vez) con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves, en tiempos muy breves, hasta encontrar la password correcta.

Los diccionarios son archivos con millones de palabras, las cuales pueden ser posibles passwords de los usuarios. Este archivo es utilizado para descubrir dicha passworden pruebas de fuerza bruta. Actualmente es posible encontrardiccionarios de gran tamaño orientados, incluso, a un área específica de acuerdo al tipo de organización que se este

Contraseñas: se roban cada vez más aunque sean más complejas

Hace poco tiempo, en el mes de agosto de 2014, en el diario La Nación, salió publicado un articulo sobre el robo de contraseñas, y del mismo surge que durante la conferencia de seguridad Black Hat, que se realizó en Las Vegas, EEUU, recientemente, la compañía estadounidense Hold Security dio a conocer una cifra insólita. Un grupo de delincuentes informáticos rusos se habrían robado 1200 millones de contraseñas y 500 millones de direcciones de correo electrónico.

El número supera todas las marcas anteriores y, si es cierto, se convierte en la mayor sustracción de datos de la historia. Como era de prever, la noticia no sólo encendió todas las alarmas, sino que también sembró escepticismo. Para el célebre criptógrafo Bruce Schneier, todo el asunto parece más una campaña mediática de Hold Security que

el reporte del robo del siglo. Por su parte, el respetado experto en seguridad Brian Krebs cree que el asalto de verdad existió, más allá de la sospechosa falta de detalles técnicos y metodológicos aportados por Hold Security.

Casi cada semana los datos sensibles de miles de usuarios son hurtados de sitios web. En ocasiones las víctimas se cuentan por millones. El 3 de octubre de 2013 la compañía Adobe, creadora del Photoshop, anunció que le habían hurtado unos 3 millones de contraseñas. El número trepó en los días siguientes a 152 millones. Casi todas las compañías con algún servicio en Internet han padecido este flagelo, desde gigantes como Sony y Google hasta ignotas pero cruciales agencias de pago.

Pero, el robo de 1200 millones de contraseñas no dice mucho, sin dar datos de como se produjo, que medidas de seguridad tenían ellos en salvaguarda de estas cntraseñas, tampoco especificaron cuánto se demoró en obtener esa cantidad de contraseñas, ni qué sitios fueron afectados y, sobre todo, qué proporción de esas claves estaban en texto plano (esto es, legibles de inmediato) o encriptadas (usando lo que se conoce como función hash).

Hay casi 3000 millones de personas conectadas a Internet y más de 1000 millones de sitios, con el número de páginas web individuales en el orden de decenas de billones. Para los grandes robos de datos, los criminales infectan cientos o miles de computadoras de particulares para incorporarlas a una red robot (o botnet) que busca de forma autónoma sitios que expongan alguna vulnerabilidad.
En el caso de los delincuentes rusos, habrían explotado una falla llamada Inyección SQL. Con el tiempo suficiente y una botnet poderosa, la cifra de 1200 millones de contraseñas es menos impresionante de lo que parece a primera vista.

DELITO EN ALZA

Pero un dato surge claro de las estadísticas. Esta clase de filtraciones está creciendo de forma alarmante. Santiago Pontiroli, analista de seguridad de la compañía KasperskyLabexpresa *"En estos últimos años el robo de contraseñas ha crecido, principalmente porque aún es la principal forma de autenticarnos y así acceder a una gran cantidad de recursos informáticos. Según nuestras estadísticas, entre 2012 y 2013*

los phishersatacaron alrededor de 102.000 personas por día, el doble de lo registrado entre 2011 y 2012. Con más del 20% de los ataques apuntando a bancos y otras instituciones financieras, los phishers no se han olvidado de las redes sociales. En 2013 la cantidad de ataques a Facebook y otras redes similares creció un 6,8%, representando el 35,4% del total".-

El phishing(virus) es una de las numerosas formas de obtener contraseñas y toma la forma de un mail con alguna advertencia grave que fuerza al usuario a ingresar en un sitio que parece la entidad financiera, pero que es en realidad una fachada engañosa donde le sustraerán sus datos sensibles.

Por su parte Ignacio Sbampato, técnico informático de la compañía de seguridad ESET de EEUU, expresa "*Nosotros no tenemos una estadística específica que diga que el robo real de contraseñas haya crecido -observa, por su parte, En general, lo que vemos es que el robo de contraseñas crece constantemente, ya sea por medio de ataques a sitios web o por el uso de malware (programas maliciosos). La razón, desde nuestro punto de vista, es que las contraseñas son la clave para utilizar los servicios, y los servicios son el objetivo de los atacantes, ya que les permiten un rédito económico directo, si el servicio es financiero, o indirecto, porque los usuarios tienden a utilizar las mismas claves en todos los servicios".*

Los usuarios de Internet se encuentran, así, en una encrucijada. Por un lado, saben que tienen que usar contraseñas robustas, es decir, capaces de resistir los intentos de adivinarlas o descifrarlas por medio de ataques de fuerza bruta. Pero no sólo esas contraseñas son difíciles de recordar, sino que, además, los delincuentes informáticos ya no necesitan quebrantarlas. Les resulta más fácil robarlas.

¿Qué hacer pues? En julio, Microsoft dio a conocer un artículo en el que aconseja reutilizar contraseñas sencillas en los sitios de poca importancia, reservando las claves fuertes sólo para el banco, el correo electrónico, Facebook y otros servicios más críticos. Aunque reñida con las buenas prácticas de seguridad, el artículo de Microsoft es más realista que las recomendaciones tradicionales.

La contraseña de nuestra cuenta de mail es particularmente sensible porque es allí donde nos envían el link para recuperar todas las otras, si nos las roban o las olvidamos. Todos

los expertos coinciden en que la contraseña de este servicio nunca debe reutilizarse en otros.

Sbampato, por su parte, opina que "*es necesario que se empiecen a utilizar métodos de autenticación más complejos, como la doble o múltiple autenticación, porque la seguridad de nombre de usuario y password ya no es suficiente"*.

LOS FRAUDES Y ATAQUES MÁS FRECUENTES

Técnicas de inteligencia, engaños y vulnerabilidades de software, todo vale

Inteligencia

El delincuente prueba combinaciones de números y palabras asociados a la víctima. Por eso no sirve usar palabras, fechas y otros datos personales.

Robo e ingeniería social

Se explotan vulnerabilidades de software que permiten extraer archivos enteros de datos de usuarios. También se usan técnicas de ingeniería social, como el phishing, para que la víctima entregue sus contraseñas voluntariamente.

Ataque de diccionario

Se intenta con las combinaciones más usadas. Por lejos, la contraseña más popular es 123456.

Ataque de fuerza bruta

Un programa prueba todas las combinaciones posibles. Este es el motivo por el que no sirven las contraseñas sencillas y de pocos caracteres.

Normas de Elección de Claves

Se debe tener en cuenta los siguientes consejos:

- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
- No usar contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, etc.).
- No utilizar terminología técnica conocida.
- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
- Deben ser largas, de 8 caracteres o más.
- Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas. Esto permite que si una password de un sistema cae no caigan todos los demás sistemas por utilizar la misma password.
- Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
- Combinar palabras cortas con algún número o carácter de puntuación: soy2_yo3
- Usar un acrónimo de alguna frase fácil de recordar: A río Revuelto Ganancia de Pescadores: ArRGdP
- Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P
- Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña: aHoelIo
- Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar
- Realizar reemplazos de letras por signos o números:

- **Algunos consejos a seguir:**
- No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente (auditoría).
- No mantener las contraseñas por defecto del sistema. Por ejemplo, cambiar las cuentas de Administrador, Root, System, Test, Demo, Guest, InetUser, etc.
- Nunca compartir con nadie la contraseña. Si se hace, cambiarla inmediatamente.

- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.
- No teclear la contraseña si hay alguien observando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.
- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "mi clave es...".
- No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente (por lo menos 5).

FIREWALLS

Quizás uno de los elementos más publicitados a la hora de establecer seguridad, sean estos elementos. Aunque deben ser uno de los sistemas a los que más se debe prestar atención, distan mucho de ser la solución final a los problemas de seguridad.

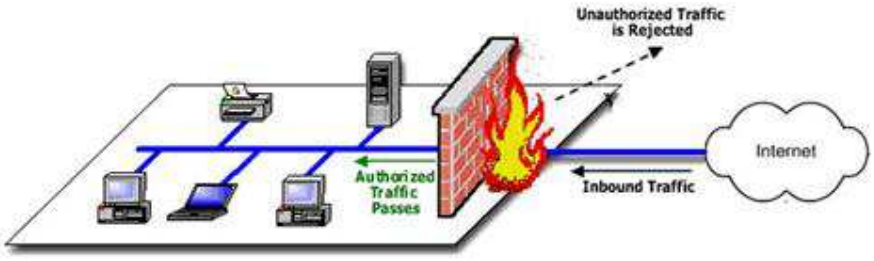
Los Firewalls están diseñados para proteger una red interna contra los accesos no autorizados. En efecto, un firewall es un *Gateway (puerta de enlace)* con un bloqueo (la puerta bloqueada solo se abre para los paquetes de información que pasan una o varias inspecciones de seguridad), estos aparatos solo lo utilizan las grandes corporaciones, por ej. Bolsa de Comercio

Una puerta de enlace es un dispositivo, con frecuencia una computadora, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.
Es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior

Un Firewall es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos

a) Todala información desde dentro hacia fuera, y viceversa, debe pasar a través de él.
b) Sólo lainformación, definida por la política local de seguridad, es permitida.



Del grafico puede observarse, el Muro Cortafuegos, sólo sirve de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.
Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red.
Se entiende que si dos Firewalls están conectados, ambos deben "hablar" el mismo método de encriptación-desencriptación para entablar la comunicación

Restricciones en el Firewall

La parte más importante de las tareas que realizan los Firewalls, la de permitir o denegar determinados servicios, se hacen en función de los distintos usuarios y su ubicación:

- Usuarios internos con permiso de salida para servicios restringidos: permite especificar una serie de redes y direcciones a los que denomina **Trusted (validados)**. Estos usuarios, cuando provengan del interior, van a poder acceder a determinados servicios externos que se han definido.
- Usuarios externos con permiso de entrada desde el exterior: este es el caso más sensible a la hora de vigilarse. Suele tratarse de usuarios externos que por algún motivo deben acceder para consultar servicios de la red interna.

También es habitual utilizar estos accesos por parte de terceros para prestar servicios al perímetro interior de la red. Sería conveniente que estas cuentas sean activadas y desactivadas bajo demanda y únicamente el tiempo que sean necesarias.

Beneficios de un Firewall

Los Firewalls manejan el acceso entre dos redes, y si no existiera, todas las computadoras de la red estarían expuestas a ataques desde el exterior. Esto significa que la seguridad de toda la red, estaría dependiendo de qué tan fácil fuera violar la seguridad local de cada máquina interna.
El Firewall es el punto ideal para monitorear la seguridad de la red y generar alarmas de intentos de ataque, el administrador será el responsable de la revisión de estos monitoreos.

Otra causa que ha hecho que el uso de Firewalls se haya convertido en uso casi imperativo es el hecho que en los últimos años en Internet han entrado en crisis el número disponible de direcciones IP, esto ha hecho que las intranets adopten direcciones sin clase, las cuales salen a Internet por medio de un "traductor de direcciones", el cual puede alojarse en el Firewall.

Los Firewalls también son importantes desde el punto de vista de llevar las estadísticas del ancho de banda "consumido" por el tráfico de la red, y que procesos han influido más en ese tráfico, de esta manera el administrador de la red puede restringir el uso de estos procesos y economizar o aprovechar mejor el ancho de banda disponible.

Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad o para albergar los servicios WWW y FTP brindados.

Limitaciones de un Firewall

La limitación más grande que tiene un Firewall sencillamente es el hueco que no se tapa y que coincidentemente o no, es descubierto por un intruso. Los Firewalls no son

sistemas inteligentes, ellos actúan de acuerdo a parámetros introducidos por su diseñador, (programador) por ende si un paquete de información no se encuentra dentro de estos parámetros como una amenaza de peligro simplemente lo deja pasar. Más peligroso aún es que ese intruso proceda abriendo un hueco diferente y borre las pruebas o indicios del ataque original.

Otra limitación es que el Firewall "NO es contra humanos", es decir que si un intruso logra entrar a la organización y descubrir passwords o los huecos del Firewall y difunde esta información, el Firewall no se dará cuenta.

El Firewall tampoco provee de herramientas contra la filtración de software o archivos infectados con virus, aunque es posible dotar a la máquina, donde se aloja el Firewall, de antivirus apropiados.

Finalmente, un Firewall es vulnerable, NO protegea los usuarios que están dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna. Como moraleja: "cuanto mayor sea el tráfico de entrada y salida permitido por el Firewall, menor será la resistencia contra los paquetes externos. El único Firewall seguro (100%) es aquel que se mantiene apagado" (1)

Cómo implementar una política de seguridad

Generalmente, la seguridad de los sistemas informáticos se concentra en garantizar el derecho a acceder a datos y recursos del sistema configurando los mecanismos de autentificación y control que aseguran que los usuarios de estos recursos sólo posean los derechos que se les han otorgado.

Los mecanismos de seguridad pueden sin embargo, causar inconvenientes a los usuarios. Con frecuencia, las instrucciones y las reglas se vuelven cada vez más complicadas a medida que la red crece. Por consiguiente, la seguridad informática debe estudiarse de modo que no evite que los usuarios desarrollen usos necesarios y así puedan utilizar los sistemas de información en forma segura.

Por esta razón, uno de los primeros pasos que debe dar una institución es definir una política de seguridad que pueda implementar en función a las siguientes cuatro etapas:

1) Identificar las necesidades de seguridad y los riesgos informáticos que enfrenta la institución así como sus posibles consecuencias
2) Proporcionar una perspectiva general de las reglas y los procedimientos que deben implementarse para afrontar los riesgos identificados en los diferentes departamentos de la institución
3) Controlar y detectar las vulnerabilidades del sistema de información, y mantenerse informado acerca de las falencias en las aplicaciones y en los materiales que se usan
4) Definir las acciones a realizar y las personas a contactar en caso de detectar una amenaza

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

En este sentido, no son sólo los administradores de informática los encargados de definir los derechos de acceso sino sus superiores. El rol de un administrador de informática es el de asegurar que los recursos de informática y los derechos de acceso a estos recursos coincidan con la política de seguridad definida por la organización.

Es más, dado que el/la administrador/a es la única persona que conoce perfectamente el sistema, deberá proporcionar información acerca de la seguridad a sus superiores, eventualmente aconsejar a quienes toman las decisiones con respecto a las estrategias que deben implementarse, y constituir el punto de entrada de las comunicaciones destinadas a los usuarios en relación con los problemas y las recomendaciones de seguridad.

La seguridad informática de una institución/organización depende de que los usuarios aprendan las reglas a través de sesiones de capacitación y de concientización. Sin embargo, la seguridad debe ir más allá del conocimiento de los usuarios y cubrir las siguientes áreas:

1) Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la institución y al uso de los empleados
2) Un procedimiento para administrar las actualizaciones
3) Una estrategia de realización de copias de seguridad (backup) planificada adecuadamente
4) Un plan de recuperación luego de un incidente
5) Un sistema documentado actualizado

Las causas de inseguridad

Generalmente, la inseguridad se puede dividir en dos categorías:

1) Un estado de inseguridad activo; es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita)
2) Un estado de inseguridad pasivo; es decir, la falta de conocimiento de las medidas de seguridad disponibles (por ejemplo, cuando el administrador o usuario de un sistema no conocen los dispositivos de seguridad con los que cuentan)

Encriptación

Encriptación es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozca los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

El término encriptación es traducción literal del inglés y no existe en el idioma español, la forma más correcta de utilizar este término sería Cifrado.

Opcionalmente puede existir además un proceso de desencriptación a través del cual la información puede ser interpretada de nuevo a su estado original.

Aunque existen métodos de encriptación que no pueden ser revertidos.

Criptología

La encriptación como proceso forma parte de la criptología, ciencia que estudia los sistemas utilizados para ocultar información, La criptología es la ciencia que estudia la

transformación de un determinado mensaje en un código de forma tal que a partir de dicho código solo algunas personas sean capaces de recuperar el mensaje original.

Usos de las Encriptación

Algunos de los usos más comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas crédito, reportes administrativos contables y conversaciones privadas, entre otros.

Métodos de Encriptación

Para poder encriptar un dato, se pueden utilizar tresprocesos matemáticos diferentes.- Los algoritmos HASH, los simétricos y los asimétricos.

Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

Criptografía de Clave Secreta o Simétrica

Utilizan una clave con la cual se encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma .clave, es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores

Los Criptosistemas de clave secreta se caracterizan porque la clave de cifrado y de la descifrado es la misma, por tanto la robustez del algoritmo recae en mantener el secreto de la misma.

Sus principales características son:

-Rápidos y fáciles de implementar

-clave de cifrado y descifrado son la misma

-cada par de usuarios tiene que tener una clave secreta compartida

-una comunicación en la que intervengan múltiples usuarios requiere de muchas claves secretas distintas.

Algoritmos Asimétricos (RSA)

Requieren dos claves, una privada (única y personal, solo conocida por su dueño) y la otra llamada pública, ambas relacionadas por una fórmula matemática compleja, imposible de reproducir.

El concepto de criptografía de clave pública fue introducido por WhitfieldDiffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. El usuario, ingresando su PIN genera clave Públicas y Privadas necesarias. La clave pública podrá ser distribuida sin ningún inconveniente entre todos los usuarios.

Firma Digital:

La firma digital permite garantiza algunos conceptos de seguridad y son importantes al utilizar documentos en formato digital, tales como identidad o autenticidad, integridad y no repudio. El modo de funcionamiento es similar a lo explicado para los algoritmos de encriptación, se utilizan también algoritmos de clave pública, aplicados en dos etapas.

Ventajas ofrecidas por la firma Digital

- **Integridad de la información**: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor control de integridad, el receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.
- **Autenticidad del origen del mensaje**: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.
- **No repudio del origen**: el no repudio del origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje , transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Encriptar datos en un PDA.

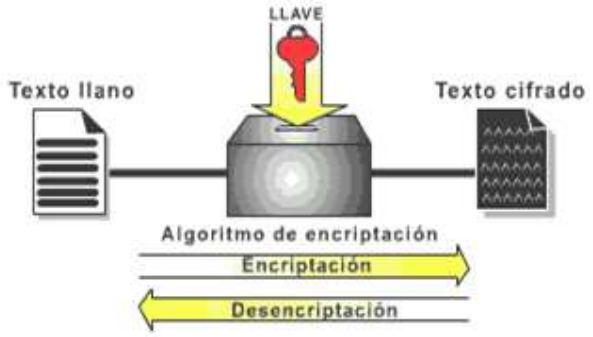
La importancia de tener nuestros datos a salvo de miradas extrañas o tener un mínimo de privacidad se ha convertido en un tema muy importante. Los PDAs son muchas veces usados como pequeñas oficinas portátiles donde se guardan datos de gran valor y donde es de gran importancia tener estos datos protegidos. Muchos usuarios PDA por comodidad no protegen el acceso de inicio con una clave, imagínense en caso de pérdida del aparato o descuido poder dejar estos datos confidenciales en manos ajenas a las nuestras. Para solucionar este problema o tener cierto grado de seguridad, es muy importante poder encriptar nuestros datos.

Encriptación de Ficheros:

Windows XP profesional nos da una alternativa para poder proteger estos datos y prevenir su pérdida. El Encripting File System (EFS) en el encargado de codificar los ficheros. Estod Ficheros solo se pueden leer cuando el usuario que los ha creado hace "logon" en su maquina (con lo cual, presumiblemente, nuestra password será una pasword robusta). De hecho, cualquiera que acceda a nuestra máquina, no tendrá nunca acceso a nuestros ficheros encriptados aunque sea un administrador del equipo.

Tipos de Cifrados

Cifrado es otro nombre que se le da al proceso de encriptación. El propósito de un cifrado es tomar datos sin encriptar, llamado texto claro o plano, y producir una versión encriptada del mismo. Existen dos clases de cifrad: Cifrado de Flujo de datos y Cifrado de bloques.



***Cifrado de flujo de datos*:** En el cifrado por flujo de datos encriptan un bit de texto en claro por vez. El ejemplo más simple de cifrado por flujo de datos es el que consiste en combinar los datos, un bit a la vez, con otro bloque de datos llamado pad. Los cifrados por flujo de datos funcionan realmente bien con datos en tiempo real como voz y video.

Cifrado por bloques: operan sobre bloques de tamaño mayor que un bit del texto en claro y producen un bloque de texto cifrado, generalmente los bloques de salida son del mismo tamaño que los de la entrada. El tamaño del bloque debe ser lo suficientemente grande como para

Antivirus

*Los **antivirus*** son herramientas simples; cuyo objetivo es detectar y eliminar virus informáticos. Nacieron durante la década de 1980.

• Un virus informático ocupa una cantidad mínima de espacio en disco (el tamaño es vital para poder pasar desapercibido), se ejecuta sin conocimiento del usuario y se dedica a auto-replicarse, es decir, hace copias de sí mismo e infecta archivos, tablas de partición o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible

• Básicamente, el propósito de un virus es provocar daño en el equipo infectado.

• Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes, así como los scripts y programas que pueden ejecutarse en un navegador web (ActiveX – Java – JavaScript)

.

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado las funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística) o la verificación contra virus en redes de computadoras. Actualmente existe una nueva tecnología basada en Inteligencia artificial llamada TruPrevent que cuenta con la capacidad de detección de virus desconocidos e intrusos.

Los antivirus son esenciales en sistemas operativos cuya seguridad es baja, como Microsoft Windows, pero existen situaciones en las que es necesario instalarlos en sistemas más seguros, como Unix y similares.

Con tantos software malignos dando vuelta por internet, se hace necesario disponer de un buen antivirus que nos proteja continuamente.

Copias de Seguridad/Backups

Incluso el sistema de seguridad más sofisticado no puede garantizar al cien por ciento una protección completa de los datos. Un pico o una caída de tensión pueden limpiar en un instante hasta el dato más cuidadosamente guardado.

Un UPS(Sistema de alimentación ininterrumpidas) puede proteger a las computadoras contra la perdida de datos durante una caída de tensión, los más baratos pueden emplearse en las casas para apagones de corta duración. Los protectores de sobrecarga no sirven durante un apagón, pero si protegen los equipos contra los dañinos picos de tensión, evitando costosas reparaciones posteriores.

Por su puestos los desastres aparecen de forma muy diversas, Los sabotajes, los errores humanos, los fallos de la máquina, el fuego, las inundaciones, los rayos y los terremotos pueden dañar o destruir los datos de la computadora además del hardware

Cualquier sistema de seguridad completo debe incluir un plan de recuperación en el caso de producirse un desastre. En mainframes y PC, lo mejor, además de ser lo más utilizado, es llevar a cabo copias de seguridad regulares.

Las copias de seguridad son una manera de proteger la inversión realizada en los datos. Las pérdidas de información no es tan importante si existen varias copias resguardadas

La copia de seguridad es útil por varias razones:

- Para restaurar un ordenador a un estado operacional después de un desastre (copias de seguridad del sistema)
- Para restaurar un pequeño número de ficheros después de que hayan sido borrados o dañados accidentalmente (copias de seguridad de datos).
- En el mundo de la empresa, además es útil y obligatorio, para evitar ser sancionado por los órganos de control en materia de protección de datos .

Normalmente las copias de seguridad se suelen hacer en cintas magnéticas, si bien dependiendo de lo que se trate podrían usarse disquetes, CD, DVD, Discos Zip, Jaz o magnéticos-ópticos, pen drivers o pueden realizarse sobre un *centro de respaldo remoto* propio o vía internet.

La copia de seguridad puede realizarse sobre los datos, en los cuales se incluyen también archivos que formen parte del sistema operativo. Así las copias de seguridad suelen ser utilizadas como la última línea de defensa contra pérdida de datos, y se convierten por lo tanto en el último recurso a utilizar.

Las copias de seguridad en un sistema informático tienen por objetivo el mantener cierta capacidad de recuperación de la información ante posibles pérdidas. Esta capacidad puede llegar a ser algo muy importante, incluso crítico, para las empresas. Se han dado casos de empresas que han llegado a desaparecer ante la imposibilidad de recuperar sus sistemas al estado anterior a que se produjese un incidente de seguridad grave

Software de copias de seguridad

Existen una gran gama de software en el mercado para realizar copias de seguridad. Es importante definir previamente los requerimientos específicos para determinar el software adecuado.

Entre los más populares se encuentran ZendalBackupCobian, SeCoFi, CopiaData y NortonGhost.

Afirmaciones erróneas comunes acerca de la seguridad informática

1) **Mi sistema no es importante para un cracker**

Esta afirmación se basa en la idea de que no introducir contraseñas seguras en una empresa no entraña riesgos pues ¿quién va a querer obtener información mía?. Sin embargo, dado que los métodos de contagio se realizan por medio de programas *automáticos*, desde unas máquinas a otras, estos no distinguen buenos de malos, interesantes de no interesantes, etc. Por tanto abrir sistemas y dejarlos sin claves es facilitar la vida a los virus.

El término hacker: es una persona que sólo desea conocer el funcionamiento interno de los sistemas informáticos, ayudando a mejorarlos en el caso de que detecte fallos en su seguridad. Sin embargo, un 'hacker' deja de serlo cuando provoca daños y su acción es malintencionada: en ese momento pasa a ser un 'cracker'.

Para un 'hacker', el objetivo es saltar los sistemas de seguridad de los servidores de Internet para llegar hasta su interior, pero, una vez dentro, no causar ningún daño. Como mucho, un 'hacker' auténtico simplemente deja una señal o "bandera" en el servidor (al estilo de "yo estuve aquí"), que sirva como prueba de que ha conseguido acceder a él.

Mediante estas señales el 'hacker' consigue dos objetivos: por un lado, demuestra ante el resto de su comunidad que ha sido capaz de acceder al servidor y, por otro, permite que los administradores del sistema vulnerado detecten el acceso al servidor, ayudándoles así a mejorar la seguridad. Es más, la mayoría de los 'hackers', tras acceder a un sistema, informan a sus propietarios de los agujeros de seguridad que tiene su servidor, para que nadie malintencionado (como un 'cracker') pueda aprovecharse a posteriori de esa vulnerabilidad.

En definitiva, la labor del 'hacker' es una lucha contra uno mismo, un "llegar más allá", poniendo a prueba sus conocimientos, destreza e inteligencia. Los propios 'hackers' se autodefinen como "unas personas interesada en explorar los detalles de los sistemas informáticos y obtener el máximo de sus capacidades, al contrario que la mayoría de los usuarios de estos sistemas, que prefieren conocer sólo lo mínimo necesario para poder trabajar con ellos"

El término cracker: Es cualquier persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

El cracker, es considerado un "vandálico virtual". Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, etc. Algunos intentan ganar dinero vendiendo la información robada, otros sólo lo hacen por fama o diversión.

Cracker es el término que define a programadores maliciosos y ciberpiratas que actúan con el objetivo de violar ilegal o inmoralmente sistemas cibernéticos, siendo un término creado en 1985 por hackers en defensa del uso periodístico del término.

2) **Algunos tipos de crackers:**

Crackers de sistemas: término designado a programadores que alteran el contenido de un determinado programa, por ejemplo, alterando fechas de expiración de un determinado programa para hacerlo funcionar como si se tratara de una copia legítima.

Crackers de Criptografía: término usado para aquellos que se dedican a la ruptura de criptografía (cracking codes)

Phreaker: cracker especializado en telefonía. Tiene conocimiento para hacer conexiones gratuitas, reprogramar centrales telefónicas, grabar conversaciones de otros teléfonos para luego poder escuchar la conversación en su propio teléfono, etc.
Ciberpunk: son los vándalos de páginas web o sistemas informatizados. Destruyen el trabajo ajeno

3) **Estoy protegido pues no abro archivos que no conozco**

Esto es falso, pues existen múltiples formas de contagio, además los programas realizan acciones sin la supervisión del usuario poniendo en riesgo los sistemas.

4) **Como tengo antivirus estoy protegido**

En general los programas antivirus no son capaces de detectar todas las posibles formas de contagio existentes, ni las nuevas que pudieran aparecer conforme los ordenadores aumenten las capacidades de comunicación, además los antivirus son vulnerables a desbordamiento de búfer que hacen que la seguridad del sistema operativo se vea más afectada aún.

5) **Desbordamiento de búfer:** es un error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos, sobrescribiendo de esta manera otras zonas de memoria. Esto se debe en general a un fallo de programación.

6) **Como dispongo de un firewall no me contagio**

Esto únicamente proporciona una limitada capacidad de respuesta. Las formas de infectarse en una red son múltiples. Unas provienen directamente de accesos al sistema (de lo que protege un firewall) y otras de conexiones que se realizan (de las que no me protege). Emplear usuarios con altos privilegios para realizar conexiones puede entrañar riesgos, además los firewalls de aplicación (los más usados) no brindan protección suficiente contra el spoofing.

7) **Spoofing**, en términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Recomendaciones

- **Actualice regularmente su sistema** operativo y el software instalado en su equipo, poniendo especial atención a las actualizaciones de su navegador web. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, le ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.
- **Instale un Antivirus** y actualícelo con frecuencia. Analice con su antivirus todos los dispositivos de almacenamiento de datos que utilice y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.
- **Instale un Firewall** o Cortafuegos con el fin de restringir accesos no autorizados de Internet.
- **Utilice contraseñas seguras**, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.
- **Navegue por páginas web seguras y de confianza**. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet
- **Ponga especial atención en el tratamiento de su correo electrónico**, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc.
- **No abra mensajes de correo de remitentes desconocidos.**
- **Desconfíe de aquellos e-mails en los que entidades bancarias,** compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
- **No propague aquellos mensajes de correo con contenido dudoso y que le piden ser reenviados a todos sus contactos.** Este tipo de mensajes, conocidos como hoaxes, pretenden avisar de la aparición de nuevos virus, transmi- tir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc.
- En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la **seguridad de su equipo informático**, para tratar de evitarlas o de aplicar la solución más efectiva posible.

La tiranía de la era digital amenaza el espíritu crítico

¿Hasta dónde la Red es virtuosa en sí misma y hasta dónde encierra efectos colaterales, contradicciones, toxicidades complejas de difícil discernimiento a simple vista

Preocupaciones como las que recoge esta pregunta abundan en un libro de no muy lejana aparición titulado *Superficiales*, cuyo autor, Nicholas Carr, periodista estadounidense, concluye que los beneficios de Internet, siendo innegables, no se alcanzan sin un costo elevado. Asegura que es ingenuo suponer, que la cultura digital es inofensiva.

La Red, advierte Carr, conspira seriamente contra la concentración y la profundidad. Contra atributos de la subjetividad, en suma, que son fundamentales para entender al hombre como aún lo hacemos.

La relación de la literatura con la función innovadora de las tecnologías ofrece, sin embargo, distintos ángulos valorativos que impiden diagnosticar de un único modo los efectos de ese vínculo. Ya se lo nota a fines del siglo XIX por lo menos en dos grandes escritores.

Hay un texto de Friedrich Nietzsche, fechado en el año 1879, en el que el filósofo admite que cuando llegó a sus manos una máquina de escribir, su prosa cambió y se hizo más telegráfica. El empleo de la mecanografía había alterado la cadencia habitual de su enunciación escrita, pero, en compensación, le había dado acceso a otra, inesperada y convincente.

Marcel Schowb, narrador notable, prevé en un artículo de 1891 que las consecuencias del creciente empuje tecnológico no tardarían en hacerse sentir en todo. Y agradece a ese fenomenal invento que es el fonógrafo la posibilidad de haber podido preservar la voz del poeta Robert Browning. Admite, no obstante, que en su tiempo impera todavía una marcada resistencia a la incorporación de los aportes de la tecnología a los hábitos vigentes en el campo de la comunicación. "Hasta el presente, el fonógrafo no ha entrado en nuestras costumbres, dormita; pero una tremenda revolución de esas costumbres se prepara para el día en que con él comience una nueva conquista de Europa y América. Aquello que detenía hasta el presente el auge del fonógrafo y del teléfono era la resistencia del auditor a añadir instrumentos a su oreja, a hablarles a instrumentos."

Hoy muchos de los recursos ofertados por la tecnología forman parte, incluso, de nuestro organismo. Es bien sabido que la tecnología científica avanza a paso redoblado en el proceso de reemplazo de lo natural por lo artificial.

El hecho inspiró uno de los libros más penetrantes sobre el tema: *"El intruso"* de Jean-Luc Nancy. El ensayista francés se pregunta si aún cabe seguir hablando de nuestro cuerpo -poblado de piezas mecánicas que reemplazan a las originarias- como de un cuerpo "propio". Pero ¿podría afirmarse, en un orden análogo, que las nuevas tecnologías han incidido sobre la escritura como para hacer de ella algo distinto de lo que fue hasta aquí?

"Siempre inventamos las mismas fábulas -ha dicho Jorge Luis Borges-. Siempre repetimos los mismos cuentos con pequeñas variaciones, con entonaciones distintas. Y eso es lo que se espera de la literatura de cada época, que repita las mismas fábulas con una muy ligera variación."

Las fábulas son incesantemente las mismas porque los conflictos a los que remite la literatura son irreductibles. En esa medida, no resultan renovables. Puede decirse, en consecuencia, que la literatura es conservadora en cuanto a los problemas que plantea, y obligadamente innovadora en cuanto a sus argumentos y estrategias discursivas. Cada época cuenta con su escenografía propia y exige otros modos de enunciación.

Creo, por lo tanto, que las innovaciones tecnológicas no alteran los fines de la escritura aunque modifiquen sus modos y tiempos de transmisión. Los cambios tecnológicos no inciden sobre los objetivos fundamentales que ella persigue desde la remota aurora de la poesía, las novelas, los documentales, etc.

Su propósito ha sido y será siempre pensar con emoción, relatar una historia para que ella sea habitada por quien no la vivió, hacer de lo singular algo revelador para muchos.

¿Cuál podría ser la incidencia negativa de los cambios tecnológicos sobre la práctica de la escritura? No son pocos ni irrelevantes los que aseguran que la facultad de memorizar se encuentra amenazada por la tecnología de punta empleada en la comunicación. "Hacia mediados del siglo XX -escribe Nicholas Carr-, la memorización había comenzado a caer en desgracia." La memoria biológica es radicalmente diferente de la memoria informática. Según KobiRosenblum, jefe del Departamento de Neurobiología y Etología de la Universidad de Haifa decía: "Mientras que el llamado cerebro artificial absorbe la información e inmediatamente la guarda en su memoria, el cerebro humano sigue procesándola mucho después de haberla recibido, y la calidad de los recuerdos

depende de cómo se procese esa información. La memoria biológica está viva. La memoria informática, no".

Por su parte Carr infiere: "Lo que da a la memoria real su riqueza y su carácter, por no hablar de su misterio y su fragilidad, es su contingencia. Existe en el tiempo, cambiando a medida que el tiempo cambia. La memoria biológica se encuentra en perpetuo estado de renovación. La memoria almacenada en una computadora, por el contrario, adopta una forma binaria y estática. La Web es una tecnología de olvido. Y gracias una vez más a la plasticidad de nuestras vías neuronales, cuanto más usamos la Web, más entrenamos nuestro cerebro para distraerse, para procesar la información muy rápidamente y de manera muy eficiente, pero sin atención sostenida. Esto ayuda a explicar por qué a muchos de nosotros nos resulta difícil concentrarnos incluso cuando estamos lejos de nuestros ordenadores. Nuestro cerebro se ha convertido en un experto en olvido, un inepto para el recuerdo".

La memoria es, pues, una experiencia personal sujeta al tiempo, al efecto de la temporalidad sobre quien se sabe tiempo. En la medida en que alguien se reconoce afectado por el tiempo que lo constituye, vulnerado por él, puede pronunciarse como escritor, puede ganar cuerpo en la literatura.

El desarrollo desbordante de la tecnología ha alentado en el hombre la presunción de que el progreso que ella le depara, por ser ilimitado, puede liberarlo de su finitud, de su inscripción en la experiencia del límite, de su sujeción al escenario de la insuficiencia. Bien se sabe que la aspiración a lo ilimitado no es un anhelo surgido en la modernidad ni las consecuencias del desenfreno posesivo un hecho catastrófico reciente. Pero la desmesura moderna tiene formas específicas. Ellas configuran lo nefasto de nuestro tiempo y eso es cada vez más evidente, aunque la razón instrumental se empeñe en negarlo y encubrirlo.

Veámoslo en un orden que excede el campo de la escritura pero al que ésta no puede ni quiere permanecer ajena.

Advierte HaraldWelzer en su libro Guerras climáticas que los recursos ambientales extenuados y envilecidos por obra de una explotación salvaje e irresponsable acotan dramáticamente el porvenir de nuestra especie. Hacia mediados del siglo actual habrá en la Tierra 9000 millones de personas, pero los recursos disponibles ofrecidos por el medio ambiente para asegurar su supervivencia habrán decrecido en forma inversamente proporcional al aumento de la población.

Las nuevas tecnologías no sólo afianzan la supremacía del hombre en la Tierra; también debilitan su auto comprensión y la comprensión del planeta donde vive, al estar al servicio de una voluntad de poder que no tolera restricciones.

Por eso, la pregunta de fondo sobre las nuevas tecnologías nada tiene que ver con su eficiencia objetiva o su valor intrínseco. Sí, en cambio -y mucho-, con la índole de quien la emplea. Entre un hacha de piedra del paleolítico y un teléfono móvil hay incontables siglos de distancia. Pero no necesariamente los hay entre aquel hombre primitivo y el de nuestro tiempo.

Conclusiones - Ponencia

Si bien día a día aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las personas. En consecuencia, se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas.

- Es necesario mantener un estado de alerta y actualización permanente: la seguridad informática es un proceso continuo que exige aprender sobre las propias experiencias.
- Las instituciones no pueden permitirse considerar la seguridad informática como un proceso o un producto aislado de los demás. La seguridad informática tiene que formar parte de las instituciones.
- Debido a las constantes amenazas en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.
- Los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger.- No importando los procesos y la tecnología, finalmente el evitar los

ataques a la seguridad queda en manos de los usuarios, conforme las precauciones que en cada caso impongan a sus archivos y bases de datos-.

- Es importante tener en cuenta la inmutabilidad de las bases informáticas de cada sistema, ya que los cerebros artificiales no funcionan, como el cerebro del hombre, que constantemente trae nuevas ideas, cambia las anteriores, y está en permanente actividad. La inteligencia artificial de las nuevas tecnologías de la era digital, deben ser permanente actualizadas, y verificarse su contenido a fin de que no colisione con los cambios de las normativas, por falta de actualización, e incorporar a las mismas las nuevas propuestas de la mente humana.- La memoria RAM o memoria digital, fuere cual fuere, siempre es estática; la memoria de ser humano es dinámica y creadora de los contenidos de la memoria digital. Por ello la era digital debe estar al servicio de la humanidad, y el hombre, con su sapiencia y experiencia, captará los permanentes cambios digitales que se operen, cada una por su propia capacitación.
- El desarrollo constante de la tecnología, alienta un totalitarismo tecnocrático, que puede poner en riego la subjetividad, uno de los atributos esenciales del hombre y de su creación artística y cultural. Ante ello, debemos ser conscientes de estas amenazas y prestar atención a los cambios, para que los mismos sean en beneficio de la humanidad y no cercenen capacidades humanas en el arte y la cultura.

Bibliografía

http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica2.shtml#ixzz38sF5dzrs
http://www.monografias.com/trabajos82/la-seguridad-informatica/la-seguridad-informatica.shtml#ixzz38sESNYWO

http://www.slideshare.net/guest8d2f0a/seguridad-informatica-3261911?src=related_normal&rel=2573451

http://www.sitiosargentina.com.ar/webmaster/cursos%20y%20tutoriales/que_es_un_antivirus.htm
http://www.segu-info.com.ar/fisica/seguridadfisica.htm
http://www.segu-info.com.ar/articulos/2-porque-caen-password-clave.htm

http://www.slideshare.net/saintmanios/8-seguridad-informatica-presentation-633705
http://www.seguridad.unam.mx/eventos/admin-unam/politicas_seguridad.pdf
Texto Introducción a la informática –George Beekman
http://www.lanacion.com.ar/1718367-
http://www.lanacion.com.ar/1724518-la-tirania-de-la-era-digital-amenaza-el-espiritu-critico- Santiago Kovadloff | La Nación