LINUX

Introducción.

Linux es un sistema operativo. Tiene dos características muy peculiares que lo diferencian del resto de los sistemas que podemos encontrar en el mercado, la primera, es que es libre, esto significa que no tenemos que pagar ningún tipo de licencia a ninguna casa desarrolladora de software por el uso del mismo, la segunda, es que el sistema viene acompañado del código fuente. Su objetivo inicial es propulsar el software de libre distribución junto con su código fuente para que pueda ser modificado por cualquier persona, dando rienda suelta a la creatividad. El hecho de que el sistema operativo incluya su propio código fuente expande enormemente las posibilidades de este sistema. Este método también es aplicado en numerosas ocasiones a los programas que corren en el sistema, lo que hace que podamos encontrar muchos programas útiles totalmente gratuitos y con su código fuente. La cuestión es que, como ya mencionamos, Linux es un sistema operativo totalmente gratuito.

Las características más comunes de los sistemas operativos son la gestión de archivos, aplicaciones software y la interacción del usuario con los recursos de una PC. Linux añade dos características adicionales: es multiusuario y multitarea. Como sistema multitarea se puede pedir al sistema que realice varias tareas al mismo tiempo. Por ejemplo, se puede editar un archivo mientras se imprime otro. Como sistema multiusuario, admite que varios usuarios trabajen con el simultáneamente, cada uno interactuando con el sistema por medio de su propio terminal.
Originalmente, los sistemas operativos fueron diseñados para optimizar la eficiencia del uso del hardware, teniendo en cuenta a este último y no al usuario, por lo cual tenían tendencia a ser inflexibles.
Linux es todo lo contrario, considera al sistema operativo como un medio para proporcionar al usuario un juego de herramientas altamente efectivas, es decir, se puede programar y configurar el sistema para adecuarlo a las necesidades especificas de cada uno; podríamos decir que pasa a ser un entorno operativo.
La potencia y flexibilidad que posee Linux lo distingue de los demás sistemas operativos tradicionales como DOS o Windows.

Linux tuvo su origen como proyecto personal de , un estudiante de la universidad de Helsinki en Finlandia. Linus inspirado por su interés en Minix, un pequeño sistema Unix desarrollado por Andy Tannenbaum, se propuso a crear lo que en sus propias palabras seria un "mejor Minix que el Minix". Y después de un tiempo de trabajar por el mismo en su proyecto, realizo esta publicación en un portal de Internet:"Hola a todos los que usáis Minix. Estoy haciendo un sistema operativo -gratis- (sólo es un hobby, no será grande y profesional como GNU) para clones AT 386(486)."
En septiembre de 1991 lanzó la versión 0,01. Linux fue ampliamente distribuido por la Internet y en los años inmediatamente

posteriores varios programadores alrededor del mundo lo refinaron y le hicieron añadiduras incorporándole la mayoría de las aplicaciones y características estándar de un Unix, Construyendo así un sistema plenamente funcional.

Qué es LINUX? - Estructura Básica.

De la misma manera que el Unix, el Linux se puede dividir generalmente en cuatro componentes principales: el núcleo, el shell, el sistema de archivos y las utilidades. El núcleo es el programa medular que ejecuta programas y gestiona dispositivos de hardware tales como los discos y las impresoras. El shell proporciona una interfaz para el usuario. Recibe órdenes del usuario y las envía al núcleo para ser ejecutadas. El sistema de archivos, organiza la forma en que se almacenan los archivos en dispositivos de almacenamiento tales como los discos. Los archivos están organizados en directorios. Cada directorio puede contener un número cualquiera de subdirectorios, cada uno de los cuales puede a su vez, contener otros archivos.

Además, Linux cuenta con unos programas de software llamados utilidades que han pasado a ser considerados como características estándar del sistema. Las utilidades son programas especializados, tales como editores, compiladores y programas de comunicaciones, que realizan operaciones de computación estándar. Incluso uno mismo puede crear sus propias utilidades

Linux contiene un gran número de utilidades. Algunas efectúan operaciones sencillas: otras son programas complejos con sus propios juegos de órdenes.

El sistema de archivos de Linux organiza los archivos en directorios, de forma similar al DOS.

Linux posee un gran número de utilidades que se pueden clasificar en tres categorías: editores, filtros y programas de comunicaciones. Y a diferencia de otros sistemas operativos se distribuye de forma gratuita bajo una licencia publica de GNU de la Free Software Foundation (Fundación de programas libres) lo que básicamente significa que puede ser copiado libremente, cambiado y distribuido dejando siempre disponible el código fuente.

El software de Linux es frecuentemente desarrollado por varios usuarios que deciden trabajar conjuntamente en un proyecto. Cualquier usuario de Linux puede acceder a la localización y descargar el software.

Diseño.

Linux es un sistema operativo completo con multitarea y multiusuario. Esto significa que pueden trabajar varios usuarios simultáneamente en él, y que cada uno de ellos puede tener varios programas en ejecución.

Fue desarrollado buscando la portabilidad de los fuentes: casi todo el software gratuito desarrollado para UNIX se compila en Linux sin problemas. Y todo lo que se hace para Linux es de libre distribución.

El núcleo es capaz de emular por su cuenta las instrucciones del coprocesador 387, con lo que en cualquier 386 con coprocesador o sin él se podrán ejecutar aplicaciones que lo requieran.

Y con el de MS-DOS se podrán acceder desde Linux a los disquetes y particiones en discos duros formateados con MS-DOS.

El núcleo de Linux ha sido desarrollado para utilizar las características del modo protegido de los microprocesadores 80386 y 80486.

Cualquiera que conozca la programación del 386 en el modo protegido sabrá que este modo fue diseñado para su uso en UNIX. Linux hace uso de esta funcionalidad precisamente.

Con el fin de incrementar la memoria disponible, Linux implementa la paginación con el disco.

Puede tener hasta 256 megabytes de espacio de intercambio en el disco duro. Cuando el sistema necesita más memoria, expulsará páginas inactivas al disco, permitiendo la ejecución de programas más grandes o aumentando el número de usuarios que puede atender a la vez. Sin embargo, el espacio de intercambio no puede suplir totalmente a la memoria RAM, ya que el primero es mucho más lento que ésta.

Las funciones principales de este sistema operativo son:

Sistema multitarea. En Linux es posible ejecutar varios programas a la vez sin necesidad de tener que parar la ejecución de cada aplicación.

Sistema multiusuario. Varios usuarios pueden acceder a las aplicaciones y recursos del sistema Linux al mismo tiempo. Y, por supuesto, cada uno de ellos puede ejecutar varios programas a la vez (multitarea).

Shell's programables. Un shell conecta las ordenes de un usuario con el núcleo de Linux, y al ser programables se puede modificar para adaptarlo a tus necesidades. Por ejemplo, es muy útil para realizar procesos en segundo plano.

Independencia de dispositivos. Linux admite cualquier tipo de dispositivo (módems, impresoras) gracias a que cada una vez instalado uno nuevo, se añade al núcleo el enlace o controlador necesario con el dispositivo, haciendo que el núcleo y el enlace se fusionen. Linux posee una gran adaptabilidad y no se encuentra limitado como otros sistemas operativos.

Comunicaciones. Linux es el sistema más flexible para poder conectarse a cualquier ordenador del mundo. Internet se creó y desarrollo dentro del mundo de Unix, y por lo tanto Linux tiene las mayores capacidades para navegar, ya que Unix y Linux son sistemas prácticamente idénticos. Con Linux podrá montar un servidor en su propia casa sin tener que pagar las enormes cantidades de dinero que piden otros sistemas.

Puesta a Punto.

Operación.

La operación del sistema es cómoda, siempre y cuando se tengan los conocimientos necesarios, como conocimientos mínimos se requieren los necesarios para usar el UNÍX, el resto es sumamente fácil, ya que lo que se tiene que aprender demás es el uso de las aplicaciones que se instalarán en el sistema operativo.

Mantenimiento.

LINUX posee el ext2, éste es un sistema de archivos mucho más avanzado que el MS-DOS, con soporte de corrección y detección de errores (los cuales inician al encender la computadora después de un apagado incorrecto), compresión de archivos, mayor tolerancia a la fragmentación de archivos y con unos tiempos de respuesta muy superiores, aunque a un costo superior de utilización de memoria.

Actualización.

Las actualizaciones pueden bajarse del Internet de forma gratuita desde los sitios oficiales de Linux. La comunidad Linux es muy dinámica. Las versiones nuevas del núcleo aparecen cada pocas semanas, y otros programas se actualizan casi a menudo. Por eso, los nuevos usuarios de Linux sienten normalmente la necesidad de actualizar sus sistemas constantemente para mantener el paso de los cambios.

No sólo esto no es necesario, sino que es una pérdida de tiempo. Para mantenerse al día de todos los cambios del mundo Linux, uno debería utilizar todo su tiempo actualizando en vez de usando su sistema.

La mejor forma de actualizar el sistema es haciéndolo a mano: actualizando solo aquellos software que se sepa que hay que actualizar.

Nos encontraremos con que cuando se actualice un componente del sistema, no tienen por que fallar los demás.

En otras palabras, hay que actualizar sólo lo que necesite y cuando se tenga que hacer. No hay que actualizar sólo por el mero hecho de actualizar. Hacerlo sólo gastaría un montón de tiempo y esfuerzo intentando mantenerse al día.

El software más importante para actualizar en el sistema es el núcleo, las librerías y el compilador gcc. Estas son las tres partes esenciales del sistema, y en algunos casos cada uno depende de las otras para que todo funcione bien. Todos ellos se toman los fuentes actualizados y se compilan manualmente. La mayor parte del resto del software del sistema no necesita ser actualizado periódicamente.

Aplicaciones.

Internet es igual a UNIX y UNIX es igual a Linux. Internet esta sostenida en UNIX y millones de servidores en el mundo operan en una computadora corriendo Linux.

Ahora la madurez de 30 años de los sistemas de la familia UNIX puede estar en cualquier computadora convirtiéndola en una poderosa estación de trabajo elevando una simple PC a un nuevo rango.

Linux hereda la fortaleza de UNIX, el único y auténtico sistema operativo, que ha sido adoptado en las últimas décadas como el único sistema base por importantes compañías e instituciones a lo largo del mundo para el desarrollo del cómputo: NASA, AT&T, FBI, Netscape y Corel Computers , algunas universidades del mundo, entre otras.

Internet como servidor.

Puede configurar su sistema Linux para que funcione como servidor, proporcionando así diversos servicios Internet; todo lo que necesita es el software de servidor adecuado y una organización de directorios segura. El software de servidor FTP, Web, Gopher y WAIS puede conseguirse gratis; Puede hacer que todos los servidores Internet se ejecuten simultáneamente; funcionan como programas demonio, esperando a recibir solicitudes de sus servicios por parte de usuarios remotos y de forma que, al recibirse una petición, la atenderá al servidor correspondiente. Así un usuario remoto podría conectarse a su servidor FTP y descargar archivos, al mismo tiempo que otro usuario esta conectado a su servidor Web, viendo sus paginas Web. Dependiendo de la frecuencia con que sean solicitados los servicios de cualquiera de estos servidores, convendrá ejecutarlos directamente o bajo el control del programa demonio inetd para que sean llamados únicamente cuando se reciban solicitudes de servicios.

Redes.

Al instalar Linux su computadora se convierte al instante en un poderoso servidor de aplicaciones y operaciones. Linux realiza acciones de enrutamiento de datos, conexión simultánea con redes de diversa naturaleza así como pared de seguridad para redes locales.

Su computadora deja de ser un simple cliente y se transforma en un poderoso servidor de Internet: páginas web, correo electrónico. Aún cuando se use una simple línea telefónica.

Además puede resguardar la red local de posibles ataques externos.

Linux se auto protege; NO existen virus para Linux.

Se puede ejecutar simultáneamente aplicaciones Linux, MS Windows, MS-DOS, Amiga, Macintosh, 68K, Atari, Commodore hasta Nintendo en un mismo escritorio. Todo esto bajo el soporte de Linux.

No se requiere reiniciar el sistema apagándolo y encendiéndolo de nuevo cada vez que se realice una modificación por muy compleja que ésta sea. Los servidores Linux pueden trabajar encendidos durante años sin requerir una reiniciación.

Alta seguridad. Nada se realiza sin que el usuario no se entere. Además de mantener una estricta auditoria de la información almacenada.

Algunas de las bases de datos con las que cuenta Linux fueron creadas por universidades, por la Armada y la Defensa de los Estados Unidos.

Tiene a su disposición durante la instalación, software de la más alta calidad mundial creado por miles de instituciones de investigación científica y tecnológica y compañías del mundo como la NASA, la Universidad de Harvard, AT&T, UNAM, la Universidad Stanford, CERN, CIA.

No se requiere gastar altas sumas de dinero para crear una estación UNIX/ Linux. Un servidor mínimo completo puede trabajar bajo una x386 y desde 4 Mb de memoria, Linux revive su equipo, nunca lo deja obsoleto.

DELITOS INFORMÁTICOS

Concepto de delitos informáticos.

El delito informático implica actividades criminales que no encuadran en las figuras tradicionales como robos, hurtos, falsificaciones, estafa, sabotaje, etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

En el ámbito internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún no existe una definición de carácter universal.

Los crímenes por computadora comprenden "cualquier comportamiento criminal en el cual la computadora ha estado involucrada con material o como objeto de la acción criminal, o como mero símbolo":

Entonces podríamos decir que los delitos informáticos son aquellos que se dan con la ayuda de la informática o técnicas anexas.

En un sentido más amplio se los puede llamar "delitos electrónicos", que serian cualquier conducta criminal que en su realización hace uso de la tecnología electrónica.

A los delitos informáticos se les puede dar una forma típica y atípica, la primera serian las CONDUCTAS típicas antijurídicas y culpables en que tiene a las computadoras como instrumento o fin, y las segundas (atípicas) son las ACTITUDES ilícitas en que se tiene a las computadoras como instrumento o fin.

Sujetos.

Ahora debemos ver los sujetos involucrados en la comisión de estos delitos.

Sujeto activo.

Las personas que cometen los delitos informáticos son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y puede ocurrir que por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible.

Como el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que los diferencia entre sí la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiara que desvía fondos de las cuentas de sus clientes.

Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por poca inteligencia.

Existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad, la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, por el contrario, el autor de este tipo de delitos se considera a sí mismo "respetable", otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de al libertad.

Sujeto pasivo.

Tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones, gobiernos, etc., que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito es sumamente importante, ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

Ha sido imposible conocer la verdadera magnitud de los delitos informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables y si a esto se le suma la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar las leyes adecuadas a esta problemática, el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la

capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para destacar, investigar y prevenir los delitos informáticos.

Clasificación.
Se han dado diferentes clasificaciones sobre estos delitos, pero la mas clara es la que los clasifica sobre la base de dos criterios:
Como instrumento o medio.
Se valen de las computadoras como método o medio para la comisión del ilícito.
Como fin u objetivo.
En esta categoría van las dirigidas en contra de la computadora, accesorios o programas como entidad física.

Tipos de delitos informáticos.
El número y tipo de delitos informáticos es imposible de calcular, pero sin embargo, las Naciones Unidas han reconocido un cierto número de delitos por ejemplo:
Fraudes cometidos mediante la manipulación de computadoras.
Dentro de esta clasificación tenemos:
Caballo de Troya: De él hablaré en el punto 6) donde hablo de los hackers.

El "salame"(salami tecniques): Consiste en alterar un programa que maneja cuentas bancarias y logra que sumas casi imperceptibles de algunas de ellas (generalmente centavos), se acrediten en otras cuentas manejadas por el autor, de las que luego extrae el dinero así obtenido.
Falsificaciones informáticas.
Utilizar la computadora para falsificar documentos comerciales.
Atentados contra el software.
Accesos fraudulentos y daños a los sistemas: Valiéndose de la confianza del titular del sistema y accediendo subrepticiamente al mismo y violando las defensas existentes, puede ingresarse a los computadores y atentar el software allí contenido.
Una vez producido el acceso fraudulento al sistema se puede dar 3 situaciones:
Que el autor sólo quiera conocer los datos privados del dueño del sistema. Esta acción, la mayoría de las veces tiene implicancias únicamente civiles.
Acceder subrepticiamente a través de la computadora a documentos o informaciones de carácter político, social, militar o económico que deban permanecer secretos en función de la seguridad, de la defensa o de las relaciones exteriores de la nación.
Alterar o destruir datos de los sistemas pertenecientes a particulares o bien la información contenida en ellos.

Si nos atenemos a una interpretación estricta llegaríamos a la conclusión que acciones como introducir un virus no constituiría una conducta típica.
Modalidades más comunes de destrucción o alteración dolosa de información.

La "bomba lógica".
El virus informático.
De ellos hablaré mas adelante, en el punto 6) cuando hable de los hackers.
La "piratería informática".
Los casos de piratería de software son aquellos sobre los que existe mayor experiencia en los tribunales de nuestro país.
Si bien la reproducción ilegal y venta de programas no se encuentra tipificada en el Código Penal, la conducta de una persona que vendía software reproducido ilegalmente era atípica y, por ende, no plausible de sanción. La doctrina entiende que existen ciertas modalidades de "piratería" que deberían ser tipificadas como delitos y otras no. Por ejemplo:
Copias caseras. Con las fabricadas por los usuarios. No constituyen delitos porque por lo general no existe un fin de lucro
Copia corporativa. Se adquiere un ejemplar original para asegurarse la asistencia técnica en caso de ser necesario y a partir de ésta se fabrican copias para ser instaladas en todas las computadoras existentes en una empresa. Obviamente no constituye delito, pero si puede dar lugar a una acción civil.
Clubes de usuarios. Mediante el pago de un arancel o cuotas se pueden obtener copias en préstamo, canje o alquiler, para elaborar nuevas copias a partir de estas. Al haber un fin de lucro hay acción delictiva.

Suministro de copias como "estimulo" de venta de computadoras. Los comercios o empresas que venden hardware "cargan" en el disco rígido del comprador copias "piratas" que el usuario no tiene que comprar y así abaratan el precio final para éste. Aquí hay acción delictiva.
Copiado de fuentes. Este consiste en que empleados de una empresa obtienen una copia de un determinado software hecho a medida de ésta, lo modifican y lo venden como si fuera un desarrollo propio. También deberá ser considerado delito.

Delitos en Internet.

Si bien la Internet ayuda a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red, esta ventaja supone grandes inconvenientes.

Actualmente es está produciendo un intenso debate respecto de la necesidad de prevenir y sancionar estos malos usos de la red, hay así argumentos a favor y en contra de la creación de una legislación sobre el uso de la red.
Podríamos sistematizar los delitos cometidos en Internet en:

Acceso no autorizado.

El uso ilegítimo de passwords y la entrada en un sistema informático siguen a la autorización del propietario, aquí el bien jurídico protegido es la contraseña.

Destrucción de datos.

Son los daños causados en la red mediante la introducción de virus.
Infracción a los derechos de autor.
La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterios en el ámbito jurisprudencial. No existe una opinión uniforme sobre la responsabilidad del propietario de un servicio on -line, respecto a las copias ilegales introducidas en el sistema.
Intercepción de e-mail.
En este caso se propone una aplicación de preceptos que castigan la violación de correspondencia.

Estafas electrónicas.

La proliferación de las compras por la red permiten que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comitiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño, existiría una engaño a la persona que compra.
No existe en al actualidad una manera de prevenir totalmente este delito, años atrás se les decía a los usuarios de tarjetas de crédito que las compras realizadas en Internet, eran seguras", dado que los productos adquiridos llegaban al domicilio en donde se recibe le resumen de la tarjeta, pero actualmente se les permite a los compradores cambiar el domicilio de destino en el momento de celebrar al compra.

Transferencia de fondos.

Este esté típico caso en el que no se produce engaño a una persona determinada sino a un sistema informático.

Espionaje.

Se han dado casos de acceso no autorizado a sistemas de información gubernamentales e intercepción de correo electrónico del servicio secreto, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.
Entre los casos más famosos podemos citar el acceso al sistema informático del Pentágono y la divulgación a través de Internet de los mensajes remitidos por el servicio secreto norteamericano durante la crisis nuclear en Corea del Norte en 1994.

Terrorismo.

La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación internacional.

Narcotráfico.
Tanto el FBI como otros organismos, han alertado sobre la necesidad de medidas que permitan interceptar y decodificar los mensajes encriptados que utilizan los narcotraficantes para ponerse en contacto con los cárteles. También se ha destacado el uso de la red par la transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recorridos.

El mal uso de Internet
Uso de comerciales no éticos.
Algunas empresas no han podido escapar a la tentación de aprovechar la red para hacer una oferta a gran escala de sus productos, llevando a cabo "mailing's electrónicos". Ello, aunque no constituye una infracción, es mal recibido por los usuarios de Internet poco acostumbrados.

Actos parasitarios.
Algunos usuarios incapaces de integrarse a grupos de discusión o foros de debate on-line, se dedican a obstaculizar las comunicaciones ajenas, interrumpiendo conversaciones de forma repetida, enviando mensajes con insultos personales, etc. Aunque la mayoría de estas conductas están previstas por los suministradores del servicio on -line, existen algunos partidarios de que se establezcan normas para sancionar estos actos.

Los cyber policías.
Los EE. UU. tienen equipos de especialistas dedicados a la localización de hackers, frente a sabotajes e intervención en caso de siniestros informáticos. Por otra parte, algunas policias como el FBI Y SCOTLAND YARD disponen de unidades especiales para investigar la comisión de delito.

PIRATERÍA.

Introducción.

La propiedad intelectual desde sus orígenes ha jugado un papel importantísimo en la sociedad, puesto que constituye la manera como se protege por una parte a los autores y a todo lo relacionado con la producción de sus obras, creaciones intelectuales en los diversos aspectos y por otra parte a las invenciones en general.

El derecho de autor, a parte del valor cultural, tiene una creciente importancia en la economía de los países. En un mundo económicamente globalizado, como el actual, donde se propende a la libre circulación de las mercaderías, se vuelve imperioso proteger al derecho de autor, con lo cual no se está salvaguardando solamente un derecho humano sino también una fuente de trabajo e ingresos en general de un país.

Por consiguiente, no puede pasarse por alto un grave problema actual y latente, como constituye la Piratería o copia de las obras intelectuales que en la mayoría de las veces se la intenta justificar bajo la común versión de que la obra copiada va a ser encaminada para el exclusivo uso personal.

El delito de la piratería, se encuentra afectando además de los intereses de su autor a las leyes del comercio legítimo porque toda producción intelectual significa inversiones y divisas para el Estado y en base a ello debería propenderse a proteger y garantizar los derechos de autor en realidad.

Gracias a las facilidades que presta en la actualidad la moderna tecnología y concretamente Internet, muchos de sus usuarios se han aprovechado del mismo para realizar reproducciones de algunas obras sin permiso alguno de su autor; sobre todo en casos de obras musicales, software y obras literarias, bajo el justificativo, de que la información que obtienen de la red es solamente para su exclusivo uso personal, cosa que no siempre es verdad y que aunque lo fuese, con ello se le está ocasionando un perjuicio grave a su autor, ya que en un principio se puede decir que con contadas reproducciones el daño no es mayor, pero en la realidad, esas reproducciones llegan a multiplicarse incontrolablemente hasta el punto de que el autor puede dejar de percibir recursos por su obra o percibirlos en un porcentaje insignificante que no representen ni una mínima parte de su esfuerzo realizado.

Lo cual llega también a influir para que el autor deje de producir obras y por consiguiente dar aportes a su país y al mundo, y se dedique a otra actividad.

La reproducción de obras literarias.

La reproducción sin autorización de su autor sobre esta clase de obras, puede ser considerada como la primera en practicarse a nivel mundial. Además, con su origen se comienza a buscar una protección para el derecho de autor, debido a que con la invención de la imprenta vino la veloz reproducción de copias de cualquier libro y a un costo mucho menor del real, siendo por esta razón demandado por un número cada vez mayor de lectores.

Desde este entonces hasta la actualidad se ha constituido en una forma sumamente común de poner las obras literarias a disposición del público, debido a que estas copias no autorizadas tienen una mayor acogida por su precio bajo, con la misma calidad de la obra, lo que hacen que toda la gente pueda acceder a ellas sin importar su condición económica, debido a que los precios están a su alcance y no se vuelvan prohibitivos como los reales.

Este fue y continúa siendo el fundamento principal para justificar la piratería, ya que incluso en diversas ocasiones han surgido opiniones como por ejemplo que ahora se critica el hecho de que en la comunidad en general y sobre todo en la juventud exista un desinterés absoluto por la lectura y el mínimo tiempo que se dedica a ella, sea efecto de la coerción ejercida por escuelas y colegios.

Refiriéndonos directamente, a la reproducción literaria no autorizada en el mundo de la informática, tenemos que la forma más común constituyen las llamadas "Bibliotecas y libros digitales" existentes en Internet, donde el usuario puede no solamente leer libros completos en formato electrónico, sino que lo principal es que ese libro electrónico puede descargarse de la red e imprimirse con facilidad en cualquier impresora, así como grabarse en el disco duro con formato HTML (que es el utilizado para páginas Web, propias de Internet) y así leerlos en un procesador de texto.

El mencionado medio es utilizado no solamente para reproducciones encaminadas al uso personal sino sobre todo para obtener lucro de la venta de esas copias que por lo general es la finalidad perseguida y que da origen a la piratería, antes que al mismo uso personal.

Reproducción de música.

A la piratería fonográfica se la ha definido como las grabaciones sonoras que se realizan para reproducir un fonograma, sin el consentimiento del titular del derecho y utilizando cualquier procedimiento que disponga el pirata para luego distribuir al público esas copias y obtener una ganancia de ese proceso.

En cuanto a lo que respecta a la reproducción de cualquier clase de música disponible en el campo de la informática a través de Internet, el más famoso e inclusive polémico programa de recopilación de música de diverso tipo, denominado originalmente como "Motion Picture Experts Group" y más conocido en su abreviatura "MP3" que por sus características muy peculiares, es el que nos puede proporcionar una idea clara y concreta de lo que abarca este tipo de reproducción no autorizada, relacionada con los puntos que hemos tratado anteriormente. Además es uno de los formatos más promocionados, que habla y da lugar no sólo a la grabación de música MP3 sino a la venta de reproductores para poder escuchar su música.

El MP3.

Una de las realidades es que en los últimos tiempos ha afectado directamente al derecho de autor en relación con los fonogramas, constituye el "formato MP3" que permite escuchar toda recopilación de música con calidad de CD sin necesidad de pagar un elevado valor en la cuenta de teléfono e incluso es posible crear un disco de DVD con más de 80 horas de música.

¿Qué es?

MP3 es la abreviatura de MPEG Audio Layer 3 (sigla de Motion Picture Experts Group o Grupo de Expertos en Películas), es un conjunto de estándares para comprimir y almacenar audio y vídeo digitales.

El MP3 le da sonido con calidad de CD en un formato de archivo que no requiere más de 1MB por cada minuto de sonido, en tanto que un CD normal o un archivo de sonido con extensión WAV requiere 11MB por minuto.

Este formato fue creado por un grupo de estudiantes universitarios y de pensadores avanzados que según uno de los articulistas, decidieron no pagar más precios elevados por un CD original y crear su propio sistema de distribución de música que permite a las personas elaborar con facilidad un archivo digital de una canción desde un CD y después aprovechar Internet como medio de compartir esos archivos con personas de similares gustos, en tan solo unos minutos y en forma gratuita o por unos pocos centavos.

Este hecho, el famoso MP3 se ha convertido en uno de los formatos más requeridos por los usuarios e incluso existen invitaciones públicas, a través de anuncios publicitarios de este formato, donde se le invita al usuario a que disponga de una colección de CD’s en el disco duro de su computadora o a que grabe su música preferida en un CD.

Requerimientos.

En cuanto a los requerimientos del MP3 para reproducir sus archivos son mínimos, una configuración estándar para una computadora personal (PC):

Computadora Pentium de 166MHz (medida de almacenamiento considerable para información), placa de sonido. CD-ROM, parlantes o auriculares, entrada para audio, conexión a Internet y espacio en el disco duro para almacenar estos archivos. Que es lo más común y normal que existe en una computadora.

La pieza más importante del software del MP3 es el reproductor que codifica uno de estos archivos MP3, luego dirige el audio hacia la tarjeta de sonido y por tanto a sus bocinas.

A estos reproductores se los puede encontrar de toda clase y para toda exigencia y se les promociona al usuario a través de direcciones electrónicas donde puede encontrar un sinnúmero de cada clase, así como también descargar programas de copiado.

Legalidad o Ilegalidad.

La dudosa legalidad del MP3 ha dado lugar a críticas feroces por parte de compañías discográficas, que son quienes se ven afectadas directamente puesto que han tenido grandes pérdidas económicas desde la aparición de este formato que cada vez se va extendiendo inexorablemente.

Las compañías discográficas se han dedicado desde hace algún tiempo a trabajar con iniciativas como formatos seguros que les permite ofrecer, vender y distribuir audio mientras controlan la redistribución; para lo cual la Sociedad General de Autores y Editores ha presentado un programa "Araña" diseñado para localizar sitios con canciones MP3.

La razón de esta medida se encuentra en el hecho de que el formato MP3 se distribuye con facilidad entre quienes no les interesa respetar las leyes de derecho de autor; ya que los afectados mantienen el criterio que la múltiple reproducción en este formato no es más que una violación al derecho de autor, sin importar la finalidad a la que se dedique dicho producto.

Quienes lo defienden manifiestan que no hay legislación al respecto, lo cual si lo llevamos a la realidad es falso puesto que toda obra en general está protegida por el derecho de autor y en este caso las obras promocionadas por el MP3 no solamente son ofrecidas al público para que las escuche sino sobre todo para que las recopile en un solo CD el número de canciones que quiera y de esa forma las tenga para el uso que desee y no necesite adquirir los CD’s legítimos distribuidos por las compañías discográficas.

Con la misma finalidad de vigilancia, existen otras Asociaciones, de una de las cuales su presidente ha manifestado que "si se distribuye música sin el permiso del propietario de los derechos de autor, se está rompiendo la ley".

Incluso se ha llegado a manifestar que los archivos MP3 no son ilegales, pero que hay muchos otros que violan los derechos de autor y por ende son ilegales y a esta última categoría pertenecen casi todos los que se encuentran en los foros de discusión de MP3

Los propulsores de este formato manifiestan que "lo más probable es que nadie lo moleste siempre y cuando no distribuya ni venda copia de sus canciones en MP3".
Con todo esto se está dando a entender al público que mientras la copia sea dedicada al exclusivo uso personal, es legal.

El MP3, en estos tiempos está sirviendo además de base para nuevas creaciones dentro de la misma rama, así tenemos los lectores portátiles del MP3.

Reproducción de software.
Podemos decir que el software al ser un programa que dirige a la computadora a administrar información o a cumplir una determinada función, cuando se separa de la computadora, constituye un bien intelectual autónomo, con sus propias características.
La separación del software de la computadora, facilitó además el copiado del incorporado en soportes magnéticos y cuya reproducción es sencilla, en pocos minutos y hasta segundos, con un costo mínimo.
La reproducción informática ilegal, es una práctica muy común en las empresas, por lo general suelen comprar un paquete de software, lo cargan en su red y a continuación realizan numerosas copias ilegales que son instaladas en el resto de sus computadoras sin pagar por ello.
La reproducción de software sin autorización de su titular, se ha encontrado también en compañías y locales dedicados a la venta y distribución de computadoras nuevas, que al comercializar el aparato a sus clientes, este incluye un amplio surtido de software ilegalmente copiado.

La reproducción representa el delito de piratería, ya que quien lo comercializa está obteniendo una ganancia de la venta del material pirateado, sobre todo cuando lo hacen pasar por legal ante ingenuos compradores que ignoran la existencia de licencias de uso.
Incluso, los programas de computación ilegales pueden ser copiados y transferidos electrónicamente por Internet a otros individuos.
En lo que respecta a los afectados por la copia ilegal de programas de información, uno y de ellos y tal vez el más representativo es Microsoft, dado el volumen de su mercado que frente a la dura realidad ha sufrido considerables pérdidas.
Ante esta realidad, además de los perjudicados directos, se han unido a combatir esta clase de reproducción, grupos denominados "Brigadas Antipiratas" cuyo fin es sobre todo resguardar el patrimonio de los creadores y colaborar en el control de la producción ilegal de obras protegidas.
Pero frente a esta serie de personas, grupos, organizaciones, sociedades, seminarios, etc. que se dedican a gestionar y defender el derecho de autor, existen ciertos grupos de individuos defensores de la copia ilegal. Ellos se han pronunciado en el sentido de que las leyes reguladoras del derecho de autor son injustas y que atentan contra la libre expresión, sostienen además que exceden en su rigurosidad porque no se han actualizado respecto a la nueva tecnología y que éstas leyes al no actualizarse, lo que buscan es generar una serie de ventajas económicas que son aprovechadas por algunas corporaciones interesadas en que el derecho de autor se quede tal como está.

HACKERS.

Conceptos.

¿Qué es el hacking?

"To hack" es un verbo inglés que significa: "entrar ilegalmente a...". En el habla común entendemos hacker como alguien que destruye los ordenadores del prójimo.

Esto es una mentira. Realmente, el hacking significa una búsqueda de información a la que se debería tener acceso legalmente. Es decir, no son dañinos. Tan solo es una protesta.

El hacking empezó en los años 50' en el MIT (Massachussets Institute of Technology). Los estudiantes de este centro dedicaron un gran esfuerzo a investigar el acceso remoto a la información. Al principio, no existían leyes que les impidieran su búsqueda, pero poco a poco se fueron creando ciertas leyes que limitaban la actividad.

La importante de todo esto no está en violar las leyes, sino en conseguir información.

Hackers.

El principal objetivo de los Hackers no es convertirse en delincuentes sino "pelear contra un sistema injusto" utilizando como arma al propio sistema. Su guerra es silenciosa pero muy convincente. . Se dedican a la penetración de sistemas informáticos a través de la red. La cultura popular define a los hackers como aquellos que, con ayuda de sus conocimientos informáticos consiguen acceder a los ordenadores de los bancos y de los negociados del gobierno. Bucean por información que no les pertenece, roban software caro y realizan transacciones de una cuenta bancaria a otra.

Los 10 mandamientos del hacker.

I-. No borrar ni destrozar información del ordenador en el que se está actuando. Es la forma más fácil de indicar al Administrador del Sistema que pasa algo raro.

II-. Las únicas modificaciones de información que deben realizarse en los ficheros son aquellas que cubran las huellas que se han dejado y que nos faciliten y permitan un acceso en posteriores ocasiones. De esta forma los manejos de información que modifican son los justos para permitirnos cubrir las espaldas y tener asegurado el sistema ante nuestro acceso futuro.

III-. Completamente prohibido dejar cualquier dato que nos identifique, ya sea real o de alias, en el ordenador que se ataca. Con un solo dato ya se puede tener una pista del culpable.

IV-. La información que se distribuya no debe distribuirse a personas desconocidas. Tan solo a aquellos que son de completa confianza. Hay mucha gente que está infiltrada. Los gobiernos pagan muy bien por información sobre actividades ilegales.

V-. Con respecto a BBS's, no dejar datos reales. Como mucho indicar al Sys Op gente que pertenezca al lugar y que pueda responder por ti. Es mejor ser un perfecto desconocido.

VI-. Tanto los ordenadores gubernamentales como los proveedores de Internet, tienen una gran facilidad de recursos a la hora de localizar intrusos. Se recomiendan universidades o empresas, que aunque tengan recursos, no son tan ilimitados como los de los anteriores.

VII-. El abuso de una Blue Box puede traducirse como una captura. Es siempre aconsejable emplear métodos como los 900s o los PAD's. Una Blue Box sí es ilegal, pero un 900 es un número de teléfono normal.

VIII-. Con respecto a la información dejada en BBS's, es siempre recomendable no decir claramente el proyecto que se está realizando, sino tratar de indicarlo mostrando el problema o el sistema operativo en el que se trabaja. Todo debe hacerse mediante referencias., ya que, si no, se pueden dejar pistas de las actividades que se realizan.

IX-. El preguntar no siempre es la mejor solución a la hora de obtener información, ya que mucha gente desconfía. Responder a una pregunta a un desconocido puede provocar una multa o arresto en caso de que sea un topo.

X-. La lectura es el comienzo, aprender la técnica lo siguiente, pero hasta que no se lleva a cabo lo aprendido, no se puede decir que se sabe algo. Una vez terminado este proceso, se volverá a leer, a aprender y a practicar más.

Ataques a nuestra información, ¿ cuales son las amenazas ?

El objetivo es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar, es tan importante como saber con que soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos.

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red.

A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos ya no son novedad. Los hay prácticamente desde que surgieron las redes digitales. Los piratas de la era cibernética que se consideran como una suerte de Robin Hood modernos y reclaman un acceso libre a los medios de comunicación electrónicos.
Genios informáticos se lanzan desafíos para quebrar tal o cual programa de seguridad, captar las claves de acceso a computadoras remotas y utilizar sus cuentas para viajar por el ciberespacio, ingresar a redes de datos, sistemas de reservas aéreas, bancos, o cualquier otra "cueva" más o menos peligrosa.

Métodos y herramientas de ataque del hacker.
Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además son motivados por diversos factores. A algunos hackers los intriga el desafío, otros mas gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

Recolección de información.
Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.
Sondeo del sistema para debilitar la seguridad.
Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad.
Una vez obtenida una lista de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor en cuestión. La corrida del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema. El intruso usa la información recolectada por este tipo de rastreadores para intentar el acceso no-autorizado al sistema de la organización puesta en la mira.

Acceso a sistemas protegidos.
El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema.
Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:
Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.
Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como "caballos de Troya" protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras maquinas.
Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos, etc.

Existen determinados programas y métodos para lograr el acceso a estos sistemas:

- Caballos de Troya.

Un caballo de Troya es un programa aparentemente útil que contiene un trozo de código que hace algo no deseado.
Consiste en introducir en un sistema conocido por el autor de la maniobra y desconocido por la víctima, un programa a través del cual el autor puede acceder a ese u otros programas del usuario.
por supuesto no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto (Por ejemplo: Formatear el disco duro, modificar un fichero, sacar un mensaje, etc.).

- Bombas lógicas.

Es la alteración de un programa con la finalidad de detener el funcionamiento del sistema en el momento decidido por el autor del hecho, destruir los datos o los programas de los mismos.

Este suele ser el procedimiento de sabotaje mas comúnmente utilizado por empleados descontentos. Consiste en introducir un programa o rutina que en una fecha determinada destruirá, modificara la información o provocara el cuelgue del sistema.

- Ingeniera social.

Básicamente convencer a la gente de que haga lo que en realidad no debería. Por ejemplo llamar a un usuario haciéndose pasar por administrador del sistema y requerirle la password con alguna excusa convincente. Esto es común cuando en el Centro de Computo los administradores son amigos o conocidos.

- Difusión de virus.

Se inserta una instrucción en un programa que pasa de mano en mano entre los usuarios, produciéndose el contagio entre los equipos informáticos con la consecuente destrucción de todos o parte de los sistemas con los que opera al ingresarse una determinada instrucción o en un tiempo dado.
Un virus es parecido a un gusano, en cuanto se reproduce, pero la diferencia es que no es un programa por sí sólo, si no que es un trozo de código que se adosa a un programa legítimo, contaminándolo. Cuando un programa contaminado se ejecuta, ejecutará también el código del virus, lo que permitirá nuevas reproducciones, además de alguna acción (desde un simple mensaje inocuo hasta la destrucción de todos los archivos).
Existen distintos tipos de virus, como aquellos que infectan archivos ejecutables (.exe, .com, .bat, etc) y los sectores de boot-partition de discos y diskettes, pero aquellos que causan en estos tiempos mas problemas son los macro-virus, que están ocultos en simples documentos o planilla de cálculo, aplicaciones que utiliza cualquier usuario de PC, y cuya difusión se potencia con la posibilidad de su transmisión de un continente a otro a través de cualquier red o Internet. Y además no están atados a un sistema operativo en particular, ya que un documento de MS-Word puede ser procesado tanto en un equipo Windows 3.x/95/98, como en una Macintosh u otras.

El ataque de virus es el más común para la mayoría de las empresas, que en un gran porcentaje responden afirmativamente cuando se les pregunta si han sido víctimas de algún virus en los últimos 5 años.
Daré más información sobre los virus informáticos en el capítulo 3.

- Obtención de passwords, códigos y claves.

Este método (usualmente denominado cracking), comprende la obtención "por fuerza bruta" de aquellas claves que permiten ingresar a servidores, aplicaciones, cuentas, etc. Muchas passwords de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario, que además nunca la cambia. En esta caso el ataque se simplifica e involucra algún tiempo de prueba y error. Otras veces se realizan ataques sistemáticos con la ayuda de programas especiales y "diccionarios" que prueban millones de posibles claves hasta encontrar la password correcta.
Es muy frecuente crackear una password explotando agujeros en los algoritmos de encriptación utilizados, o en la administración de las claves por parte la empresa.
Por ser el uso de passwords la herramienta de seguridad mas cercana a los usuarios, es aquí donde hay que poner enfasis en la parte "humana" con políticas claras (como se define una password?, a quien se esta autorizado a revelarla?) y una administración eficiente (cada cuanto se están cambiando?)
No muchas organizaciones están exentas de mostrar passwords escritas y pegadas en la base del monitor de sus usuarios, u obtenerlas simplemente preguntando al responsable de cualquier PC, cual es su password?.

La inversión.
Los costos de las diferentes herramientas de protección se están haciendo accesibles, en general, incluso para las organizaciones más pequeñas. Esto hace que la implementación de mecanismos de seguridad se de prácticamente en todos los niveles. Empresas grandes, medianas, chicas y las multinacionales más grandes. Todas pueden acceder a las herramientas que necesitan y los costos van de acuerdo con la empresa.
Pero no es sólo una cuestión de costos, Los constantes cambios de la tecnología hacen que para mantener un nivel parejo de seguridad cada empresa deba actualizar permanentemente las herramientas con las que cuenta. Como los hackers mejoran sus armas y metodologías de penetración de forma incesante, el recambio y la revisión constantes en los mecanismos de seguridad se convierten en imprescindibles. Y éste es un verdadero punto crítico.

Lammers.
Este estamento es él más bajo. Los Lammers son "newbies" qué van por el mal camino. Si consiguen continuar en el Underground, se convierten en Crackers cuándo aprenden. Normalmente son personas qué encuentran nukers en alguna

página web, se los descargan y se dedican a tirar al personal de los chat. No son muy peligrosos, ya qué no saben mucho. De todas formas, son fácilmente. En el mundo de los hackers, estos usuarios no suelen durar, ya qué se van metiendo con la gente y casi siempre se encuentran con alguien qué sabe más qué ellos. En este momento su carrera de Lammer ha terminado.

Phreackers.

Los Phreackers se dedican a cualquier cosa relacionada con las líneas telefónicas. Por ejemplo, buscan maneras de llamar gratis desde las cabinas. En cierto modo también es una forma de protesta, ya que consideran gratuito el acceso a la comunicación con sus semejantes.

Crackers.

Cracker pirata.

El Cracker pirata, es inofensivo excepto para los bolsillos de los productores de video-juegos, películas, música, etc. Es el que se dedica a copiar juegos y cosas así. No es tan fácil. Alguien dirá: "Pues yo tengo grabadora y puedo copiar lo que quiera". El que diga eso seguramente no ha intentado copiar ciertos programas que tienen unos anticopy que dan miedo. Un Cracker es capaz de saltarse todos los anticopy que hay, y eso no es ningún juego de niños.

Cracker vándalo.

Este personaje es algo parecido a un "hacker dañino". Se dedica a asaltar a los navegantes, meterse en sus computadoras y destruir, sólo por el placer de hacerlo. Son peligrosos por que estos controlan bastante de computadoras y pueden generar graves problemas. Si lo comparamos con la realidad, estos serían los maleantes del ciberespacio.

SEGURIDAD

Introducción.

Vamos a hacer una distinción entre seguridad y protección. El problema de la seguridad consiste en lograr que los recursos de un sistema sean utilizados para los fines previstos. Para eso se utilizan mecanismos de protección.

Los sistemas operativos proveen algunos mecanismos de protección para poder implementar políticas de seguridad.

Los mecanismos que ofrece el sistema operativo necesariamente deben complementarse con otros de carácter externo. Por ejemplo, impedir el acceso físico de personas no autorizadas a los sistemas es un mecanismo de protección cuya implementación no tiene nada que ver con el sistema operativo.

Un aspecto importante de la seguridad es el de impedir la pérdida de información, la cual puede producirse por diversas causas: fenómenos naturales, guerras, errores de hardware o de software, o errores humanos. La solución es una sola: mantener la información respaldada, de preferencia en un lugar lejano.

Otro aspecto importante de la seguridad, es el que tiene que ver con el uso no autorizado de los recursos:

Lectura de datos.

- Modificación de datos.
- Destrucción de datos.
- Uso de recursos: ciclos de CPU, impresora, almacenamiento.

Aquí el sistema operativo juega un rol fundamental, ofreciendo mecanismos de autorización y autentificación.

Toda organización debe estar a la vanguardia de los procesos de cambio, donde disponer de información continua, confiable y en tiempo, constituye una ventaja fundamental; donde tener información es tener poder y donde la información se reconoce como:

- Crítica: indispensable para garantizar la continuidad operativa de la organización.
- Valiosa: es un activo corporativo que tiene valor en sí mismo.
- Sensitiva: debe ser conocida por las personas que necesitan los datos.

La seguridad informática debe garantizar:

- La disponibilidad de los sistemas de información.
- El recupero rápido y completo de los sistemas de información
- La integridad de la información.
- La confidencialidad de la información.
- Implementación de políticas de seguridad informática.
- Identificación de problemas.

Principios básicos para la seguridad.

Suponer que el diseño del sistema es público.

El defecto debe ser: sin acceso.

Chequear permanentemente.

Los mecanismos de protección deben ser simples, uniformes y construidos en las capas más básicas del sistema.

Los mecanismos deben ser aceptados sicológicamente por los usuarios.

Redes.

Auditoria de comunicaciones.

Ha de verse:

- La revisión de costos y la asignación formal de proveedores.
- Creación y aplicabilidad de estándares.
- Cumpliendo como objetivos de control:
- Tener una gerencia de comunicaciones con plena autoridad de voto y acción.
- Llevar un registro actualizado de módems, controladores, terminales, líneas y todo equipo relacionado con las comunicaciones.
- Mantener una vigilancia constante sobre cualquier acción en la red.
- Registrar un coste de comunicaciones y reparto a encargados.
- Mejorar el rendimiento y la resolución de problemas presentados en la red.

Para lo cual se debe comprobar:

- El nivel de acceso a diferentes funciones dentro de la red.
- Coordinación de la organización de comunicación de datos y voz.
- Deben existir normas de comunicación en:
- Uso de conexión digital con el exterior como Internet.
- La responsabilidad en los contratos de proveedores.
- La creación de estrategias de comunicación a largo plazo.
- Planificación de cableado.
- Planificación de la recuperación de las comunicaciones en caso de desastre.
- Tener documentación sobre el diagramado de la red.
- Se deben hacer pruebas sobre los nuevos equipos.
- Se deben establecer las tasas de rendimiento en tiempo de respuesta de las terminales y la tasa de errores.

Auditoria de la red física.

Se debe garantizar que exista:

- Áreas de equipo de comunicación con control de acceso.
- Protección y tendido adecuado de cables y líneas de comunicación para evitar accesos físicos.
- Prioridad de recuperación del sistema.
- Control de las líneas telefónicas.

Comprobando que:

- El equipo de comunicaciones ha de estar en un lugar cerrado y con acceso limitado.
- La seguridad física del equipo de comunicaciones sea adecuada.
- Se tomen medidas para separar las actividades de los electricistas y de cableado de líneas telefónicas.
- Las líneas de comunicación estén fuera de la vista.
- Se dé un código a cada línea, en vez de una descripción física de la misma.
- Haya procedimientos de protección de los cables y las bocas de conexión para evitar pinchazos a la red.
- Existan revisiones periódicas de la red buscando pinchazos a la misma.
- El equipo de prueba de comunicaciones ha de tener unos propósitos y funciones específicas.
- Existan alternativas de respaldo de las comunicaciones.
- Con respecto a las líneas telefónicas: No debe darse el número como público y tenerlas configuradas con retrollamada, código de conexión o interruptores.

Auditoria de la red lógica.

En ésta, debe evitarse un daño interno, como por ejemplo, inhabilitar un equipo que empieza a enviar mensajes hasta que satura por completo la red.

Para éste tipo de situaciones:

- Se deben dar contraseñas de acceso.
- Controlar los errores.
- Garantizar que en una transmisión, ésta solo sea recibida por el destinatario. Para esto, regularmente se cambia la ruta de acceso de la información a la red.
- Registrar las actividades de los usuarios en la red.
- Encriptar la información pertinente.
- Evitar la importación y exportación de datos.

En cada sesión de usuario:

- Se debe revisar que no acceda a ningún sistema sin autorización.
- Inhabilitar al usuario que tras un número establecido de veces yerra en dar correctamente su propia contraseña
- Se debe obligar a los usuarios a cambiar su contraseña regularmente.
- Las contraseñas no deben ser mostradas en pantalla tras digitarlas
- Para cada usuario, se debe dar información sobre su última conexión a fin de evitar suplantaciones.
- Inhabilitar el software o hardware con acceso libre.

- El software de comunicación, debe tener procedimientos correctivos y de control ante mensajes duplicados, fuera de orden, perdidos o retrasados.
- Se debe hacer un análisis del riesgo de aplicaciones en los procesos.
- Se debe hacer un análisis de la conveniencia de cifrar los canales de transmisión entre diferentes organizaciones.
- Asegurar que los datos que viajan por Internet vayan cifrados.

COMERCIO ELECTRÓNICO.

El comercio electrónico es cualquier actividad de intercambio comercial en la que las órdenes de compra / venta y pagos se realizan a través de un medio informático, los cuales incluyen servicios financieros y bancarios suministrados por Internet. El comercio electrónico es la venta a distancia aprovechando las grandes ventajas que proporcionan las nuevas tecnologías de la información, como la ampliación de la oferta, la interactividad y la inmediatez de la compra, con la particularidad que se puede comprar y vender a quién se quiera, y, dónde y cuándo se quiera. Es toda forma de transacción comercial o intercambio de información, mediante el uso de nueva tecnología de comunicación entre empresas, consumidores y administración pública.

El principio de comercio electrónico es: intercambio de productos digitales en una base electrónica con interacciones electrónicas.

Ventajas y oportunidades.

El comercio electrónico le permite al empresario:

- Desaparecer los límites geográficos para su negocio.
- Estar disponible las 24 horas del día, 7 días a la semana, todos los días del año.
- Reducción de un 50% en costos de la puesta en marcha del comercio electrónico, en comparación con el comercio tradicional.
- Hacer más sencilla la labor de los negocios con sus clientes.
- Reducción considerable de inventarios.
- Agilizar las operaciones del negocio.
- Proporcionar nuevos medios para encontrar y servir a clientes.
- Incorporar internacionalmente estrategias nuevas de relaciones entre clientes y proveedores.
- Reducir el tamaño del personal de la fuerza.
- Menos inversión en los presupuestos publicitarios.
- Reducción de precios por el bajo costo del uso de Internet en comparación con otros medios de promoción, lo cual implica mayor competitividad.
- Cercanía a los clientes y mayor interactividad y personalización de la oferta.
- Desarrollo de ventas electrónicas.
- Globalización y acceso a mercados potenciales de millones de clientes.
- Implantar tácticas en la venta de productos para crear fidelidad en los clientes.
- Enfocarse hacia un comercio sin el uso del papel.
- Bajo riesgo de inversión en comercio electrónico.
- Rápida actualización en información de productos y servicios de la empresa (promociones, ofertas, etc.).
- Obtener nuevas oportunidades de negocio, con la sola presencia en el mercado.
- Reducción del costo real al hacer estudios de mercado.

Seguridad en el Comercio Electrónico.

La seguridad en el comercio electrónico y específicamente en las transacciones comerciales es un aspecto de suma importancia. Para ello es necesario disponer de un servidor seguro a través del cual toda la información confidencial viaja de forma segura, esto brinda confianza tanto a proveedores como a compradores que hacen del comercio electrónico su forma habitual de negocios.

Al igual que en el comercio tradicional existe un riesgo en el comercio electrónico, al realizar una transacción por Internet, el comprador teme por la posibilidad de que sus datos personales (nombre, dirección, número de tarjeta de crédito, etc.) sean interceptados por "alguien", y suplante así su identidad; de igual forma el vendedor necesita asegurarse de que los datos enviados sean de quien dice serlos.

La seguridad total es muy cara.

Hoy es imposible hablar de un sistema 100% seguro, porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos: deben optar entre perder un negocio o arriesgarse a ser hackeadas. La cuestión es que, en algunas organizaciones puntuales, tener un sistema de seguridad muy acotado les impediría hacer más negocios.

La solución a medias, entonces, sería acotar todo el espectro de seguridad, en lo que hace a plataformas, procedimientos y estrategias. De esta manera se puede controlar todo un conjunto de vulnerabilidades, aunque no se logre la seguridad total. Y esto significa ni más ni menos que un gran avance con respecto a unos años atrás.

Microsoft desafía a hackers.

05.08.99): Microsoft le invita a probar sus habilidades como hacker mediante un sitio Web operado en un ambiente Windows 2000 y desprovisto de software Cortafuegos (Firewall). Con ello, los interesados tienen la posibilidad de irrumpir en un servidor sin ser perseguidos luego por la justicia.

La compañía informa que en todo momento el servidor tendrá instalada la última versión beta del sistema operativo Windows 2000. El desafío forma parte de las pruebas de seguridad que Microsoft realiza con el sistema operativo, que según las intenciones de la compañía ha de convertirse "en el más seguro que haya existido".

En su lista de condiciones para participar en el Hacking autorizado, la compañía sugiere a quienes logren ingresar al servidor "cambiar archivos o contenidos, aunque evitando los comentarios insolentes o groseros". De igual modo, indica que el servidor contiene una serie de mensajes ocultos, que invita a encontrar. Bajo el subtítulo "Hágalo Interesante", la compañía precisa que filtrará aquellos intentos de Hacking simple, tales como el bombardeo de paquetes tendientes a doblegar al servidor desbordando su capacidad de respuesta.

Linux desafía a hackers.

(06.08.99): Luego del desafío planteado por Microsoft a hackers interesados en poner a prueba la seguridad y presunta impenetrabilidad de Windows 2000, la compañía Linux PPC lanzó una oferta similar. El premio para quien logre violar la seguridad del servidor es… el servidor.

Para el caso de Linux PPC, se trata de un servidor operado con la instalación estándar, incluyendo Telnet y el servidor Web Apache. Desde su instalación, el martes 3, a la fecha, el servidor ha registrado 11.294 intentos infructuosos de irrupción.

El hacker que logre penetrar el servidor se llevará la máquina como premio, informa Linux PPC. La única condición será reproducir exactamente, paso a paso, el procedimiento seguido.

En la página Web creada para el concurso, J. Carr, administrador del sistema, "felicita" a los 87 habilidosos que hasta ahora han intentado realizar una conexión Telnet a la máquina pretendiendo ser el propio Carr.

VIRUS INFORMÁTICOS.

Concepto de virus informático.

Al hablar de virus en la red informática, existen muchas preguntas sin respuestas, dentro de las que se encuentran las siguientes opiniones:

- Son Programas de Computadoras
- Su principal característica es la de poder auto replicarse.
- Intentan ocultar su presencia, hasta el momento de la explosión.
- Producen efectos dañinos en el Huésped.

Si obviamos el primer punto y observamos los restantes, nos podremos dar cuenta que estas características son muy semejantes a las de un virus biológico, de ahí el nombre adoptado. Así como el cuerpo humano puede ser atacado por agentes infecciosos, también las computadoras, con emisarios infecciosos capaces de alterar el correcto funcionamiento de este e incluso provocar daños irreparables en ciertas ocasiones, es así como esta puede borrar toda la información de su disco duro, o cambiar el formato de trabajo de Word o Excel. También puede hacer que el sistema quede bloqueado o crear algunos "efectos especiales" interesantes de ver, como letras que caen de la pantalla.

Un virus informático es un programa de computadora, tal y como podría ser un procesador de textos, una hoja de cálculo o un juego. Obviamente ahí termina todo su parecido con estos típicos programas que casi todo el mundo tiene instalados en sus computadoras. 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 reproducirse, es decir, hace copias de sí mismo e infecta archivos o sectores de arranque de los discos duros y disquetes para poder expandirse lo más rápidamente posible. La propagación de estos a través de las maquinas, se puede realizar de diversas formas, por medio de disquetes o a través de las redes de comunicación que unen una serie de computadoras.

Clasificación

Dependiendo del lugar donde se alojan, la técnica de replicación o la plataforma en la cual trabajan, podemos clasificarlos en distintos tipos de virus:

- Virus de archivos
- Virus de acción directa
- Virus de sobre escritura
- Virus de compañía
- Virus de Macro
- Virus del MIRC
- Virus Mutantes
- Bombas de Tiempo
- Infectores de Programas Ejecutables

Virus de archivos

Infectan archivos y tradicionalmente los tipos ejecutables COM y EXE han sido los mas afectados, aunque es estos momentos son los archivos DOC y XLS los que están en boga gracias a los virus de macro. Normalmente lo que realizan es insertar el código del virus al principio o al final del archivo, manteniendo intacto el programa infectado. Cuando se ejecuta, el virus puede hacerse residente en memoria y luego devuelve el control al programa original para que se continúe de modo normal.
Un ejemplo de estos virus es "El Viernes 13", el cual es un ejemplar representativo de este grupo.
Dentro de la categoría de virus de archivos podemos encontrar mas subdivisiones, como los siguientes:

Virus de acción directa.

Son aquellos que no quedan residentes en memoria y que se replican en el momento de ejecutarse un archivo infectado.

Virus de sobre escritura.

Corrompen el archivo donde se ubican al sobrescribirlo.

Virus de compañía.

Aprovechan una característica del DOS, gracias a la cual si llamamos un archivo para ejecutarlo sin indicar la extensión, el sistema operativo buscará en primer lugar el tipo COM. Este tipo de virus no modifica el programa original, sino que cuando encuentra un archivo tipo EXE crea otro de igual nombre conteniendo el virus con extensión COM. De manera que cuando tecleamos el nombre ejecutaremos en primer lugar el virus, y posteriormente éste pasará el control a la aplicación original.

Virus de Macro

Es una familia de virus de reciente aparición y gran expansión. Estos programas están usando el lenguaje de macros Word Basic, gracias al cual pueden infectar y replicarse a través de archivos MS-Word (*.DOC). En la actualidad esta técnica se ha extendido a otras aplicaciones como Excel.

Hoy en día son el tipo de virus que están teniendo un mayor auge debido a que son fáciles de programar y de distribuir a través de Internet. Aún no existe una concienciación del peligro que puede representar un simple documento de texto.

Virus Mutantes.

Son los que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados (Satán, Miguel Ángel, por mencionar algunos).

Bombas De Tiempo.

Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE. En espera de una fecha o una hora determinadas para "explotar". Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento, se activan cuando se ejecuta el programa que las contiene.

Infectores de programas ejecutables.

Estos son los virus mas peligrosos, porque se diseminan fácilmente hacia cualquier programa (como hojas de cálculo, juegos, procesadores de palabras).

Tipos de virus informáticos.

"**Melissa**". Es un Virus bastante conocido, utiliza los libros de direcciones de Microsoft Outlook para inundar a las computadoras de mensajes de correo electrónico, debutó en marzo de 1999. Fue uno de los virus de más rápida propagación que se conocen. Melissa destruye archivos en los discos duros de los usuarios y en las computadoras conectadas a una misma red.

"**Anna Kournikova**". Fue potencialmente tan devastador como el virus del amor y llevaba casi el mismo código. Sin embargo, la gente recibía una "carta de amor" en su buzón y la abría. La diferencia es la curiosidad, debido a que no mucha gente estuvo interesada en saber quién era "Anna Kournikova".

"**Pindonga**". Es un Virus Polimórfico residente en memoria que se activa los días 25 de febrero, 21 de marzo, 27 de agosto y 16 de septiembre, cuando ataca, borra toda la información contenida en el Disco Duro.

"**Leproso**". Creado en 1993, en Rosario, provincia de Santa Fe, se activa el día 12 de Enero (cumpleaños del autor), y hace aparecer un mensaje que dice: "Felicitaciones, su máquina está infectada por el virus leproso creado por J. P.. Hoy es mi cumpleaños y lo voy a festejar formateando su rígido.

Funcionamiento.

Hay que tener en cuenta que un virus es simplemente un programa. Por lo tanto, debemos dejar a un lado las histerias y los miedos infundados que ellos producen y al mismo tiempo ser conscientes del daño real que pueden causarnos. Para ello, lo mejor es tener conocimiento de como funcionan y las medidas que debemos tomar para prevenirlos y hacerles frente.

Proceso de infección.

Dependiendo del tipo de virus el proceso de infección varia sensiblemente.

Puede que el disco contaminado tenga un virus de archivo en el archivo FICHERO.EXE por ejemplo. El usuario introduce el disco en la computadora y mira el contenido del disco... unos archivos de texto, unas planillas de calculo, algunas imágenes... ahí esta, un ejecutable. Vamos a ver que tiene. El usuario ejecuta el programa. En ese preciso momento las instrucciones del programa son leídas por el computadora y procesadas, pero también procesa otras instrucciones que no deberían estar ahí. El virus comprueba si ya se ha instalado en la memoria. Si ve que todavía no está contaminada pasa a esta y puede que se quede residente en ella. A partir de ese momento todo programa que se ejecute será contaminado. El virus ejecutará todos los programas, pero después se copiará a sí mismo y se "pegará" al programa ejecutado "engordándolo" unos cuantos bytes. Para evitar que usuarios avanzados se den cuenta de la infección ocultan esos bytes de más para que parezca que siguen teniendo el mismo tamaño. El virus contaminará rápidamente los archivos de sistema,

aquellos que están en uso en ese momento y que son los primeros en ejecutarse al arrancar la computadora. Así, cuando el usuario vuelva a arrancar la computadora el virus se volverá a cargar en la memoria cuando se ejecuten los archivos de arranque del sistema contaminados y tomará otra vez el control del mismo, contaminando todos los archivos que se encuentre a su paso.

Propiedades de los virus.

Además de la característica principal de estos programas, que es su facultad de duplicación, existen otros muchos caracteres de los virus, como son los siguientes:

Modifican el código ejecutable: Aquí aparece el adjetivo "contagio". Para que un virus contagie a otros programas ejecutables, debe ser capaz de alterar la organización del código del programa que va a infectar.

Permanecen en la memoria de nuestra computadora: Cuando un usuario, inocente de las consecuencias, ejecuta en su ordenador un programa con virus, éste pasa a acomodarse en la memoria RAM. Esto lo hace para adueñarse de la computadora, y por así decirlo, tomar el mando.

Se ejecutan involuntariamente: Un virus sin ejecutar es imposible que dañe nuestra computadora. En ese momento está en reposo, en modo de espera, necesitado de alguien que por equivocación ejecute el programa "portador".

Funcionan igual que cualquier programa: Un virus, al ser un programa de computadora, se comporta como tal, a lo cual hay que dar gracias. Dicho programa necesita de alguien que lo ponga en funcionamiento, si no, es software inútil.

Es nocivo para la computadora: Pero esto depende del virus con el que tratemos. Podemos encontrarnos programas que destruyen parcial o totalmente la información, o bien programas que tan solo concluyen en un mensaje continuo en pantalla, aunque al final muy molesto.

Se ocultan al usuario: Claramente, el programador del virus desea que el usuario no lo advierta durante el máximo tiempo posible, hasta que aparezca la señal de alarma en nuestro ordenador. Conforme pasa el tiempo, los virus van desarrollando más y mejores técnicas de ocultamiento, pero también se van desarrollando los programas antivirus y de localización.

ANTIVIRUS.

¿Qué son los Antivirus?

Los programas antivirus son una herramienta específica para combatir el problema virus, pero es muy importante saber como funcionan y conocer bien sus limitaciones para obtener eficiencia en el combate contra los virus. Cuando se piensa en comprar un antivirus, no debe perderse de vista que debe esta bien configurado. Además, un antivirus es una solución para minimizar los riesgos y nunca será una solución definitiva, lo principal es mantenerlo actualizado. La única forma de mantener un sistema seguro es mantener el antivirus actualizado y estar constantemente leyendo sobre los virus y las nuevas tecnologías. La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Éste es el aspecto más importante de un antivirus, pero, las empresas deben buscar identificar también las características administrativas que el antivirus ofrece. La instalación y administración de un antivirus en una red es una función muy compleja si el producto no lo hace automáticamente. Es importante tener en claro la diferencia entre "detectar" e "identificar" un virus en una computadora. La detección es la determinación de la presencia de un virus, la identificación es la determinación de qué virus es. Aunque parezca contradictorio, lo mejor que debe tener un antivirus es su capacidad de detección, pues las capacidades de identificación están expuestas a muchos errores y sólo funcionan con virus conocidos.

Identificación.

El modelo más primario de las funciones de un programa antivirus es la detección de la presencia de un virus y, en lo posible, su identificación. La primera técnica que se popularizó en los productos antivirus fue la técnica de rastreo (scanning). Los rastreadores antivirus representan la mayoría de los productos de actualidad. La desventaja de los rastreadores es que éstos no consiguen reconocer los virus "desconocidos"; o sea, todo nuevo virus necesita ser descubierto y analizado antes de que un rastreador pueda reconocerlo. La velocidad de actualización de un rastreador depende en mucho de los laboratorios de cada fabricante; cuantos más laboratorios haya en el mundo, más Ingenieros Investigadores locales estarán trabajando en la localización de un virus, haciendo así un trabajo más rápido y eficiente para la solución del antivirus.
Rastrear es el método conocido para localizar un virus después de que éste haya infectado un sistema. Cabe mencionar que los rastreadores también pueden identificar los virus por nombre, mientras otros métodos no pueden.

Detección.

Debido a las limitaciones de la técnica de rastreo, los productores de programas antivirus han desarrollado otros métodos para detección de virus informáticos. Estas técnicas buscan identificar los virus por funciones básicas comunes, reconociendo el virus por su comportamiento y no por una pequeña porción de código como lo hacen los rastreadores. De hecho, esta naturaleza de procedimientos busca, de manera bastante eficiente, instrucciones potencialmente dañinas pertenecientes a un virus informático.
El método de monitoreo del sistema (también conocido como rule- based) es la mejor alternativa de protección en tiempo real para PC's individuales o para estaciones de trabajo. Estos sistemas antivirus permanecen residentes en la memoria y quedan a la expectativa en caso de actividades virulentas. Por ejemplo, si un programa en memoria intentara infectar un archivo en el disco, un producto antivirus de monitoreo de sistema percibirá dicho intento y alertará al usuario.

Limpieza

El antivirus debe ofrecer la opción de mantener una copia del archivo infectado durante la limpieza. La limpieza de un virus de un archivo puede causar algún daño y la recuperación puede no ser bien sucedida, con una copia se puede intentar una nueva limpieza o enviar el archivo para un "virus hospital" para ser limpiado por "virus doctors" (www.antivirus.com)

Actualizaciones.

El programa antivirus debe permitir una actualización automática por Internet, cuando hablo de actualización yo no estoy hablando solamente de los padrones de virus que permiten la identificación del virus por el nombre, pero es importante que el programa antivirus permita también la actualización del ejecutable de detección. Se debe verificar también cual es el período de actualización, hay virus nuevos todos los días, si la actualización tardara mucho, el sistema antivirus no podrá ser eficiente.

Medidas antivirus

Nadie que usa computadoras es inmune a los virus de computación. Un programa antivirus por muy bueno que sea se vuelve obsoleto muy rápidamente ante los nuevos virus que aparecen día a día.

- Desactivar arranque desde disquete en el setup para que no se ejecuten virus de boot.
- Desactivar compartir archivos e impresoras.
- Analizar con el antivirus todo archivo recibido por e-mail antes de abrirlo.
- Actualizar antivirus.
- Activar la protección contra macro virus del Word y el Excel.
- Sea cuidadoso al bajar archivos de Internet (Analice si vale el riesgo y si el sitio es seguro)
- No envíe su información personal ni financiera a menos que sepa quien se la solicita y que sea necesaria para la transacción.
- No comparta discos con otros usuarios.
- No entregue a nadie sus claves, incluso si lo llaman del servicio de Internet u otro.
- Enseñe a sus niños las practicas de seguridad, sobre todo la entrega de información.
- Cuando realice una transacción asegúrese de utilizar una conexión bajo SSL
- Proteja contra escritura el archivo Normal.dot
- Distribuya archivos RTF en vez de *.DOC
- Realice backups.

CONCLUSIONES.

La conclusión más importante que saqué luego de realizar este informe es casi todos los sistemas informáticos son fácilmente vulnerables para cualquier hacker, no siendo tan así las computadoras o redes que trabajan con Linux, porque como ya mencioné anteriormente "Nada se realiza sin que el usuario no se entere" y "NO existen virus para Linux".
Pero una de las ventajas más importantes es que se puede bajar gratuitamente de diversos sitios de Internet, al igual que sus respectivas actualizaciones y sobre todo que puede estar instalado simultáneamente con Windows y así poder utilizar algunas de sus aplicaciones (aunque Linux también las tiene)

Ahora, si Linux parece un sistema operativo casi perfecto ¿Por qué la mayoría de las personas y de las organizaciones usan Windows y no Linux?
Quizás una de las causas sea su operabilidad y que viene instalado con cualquier equipo de computación que compramos, pero creo que la mas importante es que Windows está muy bien ubicado en la mente de las personas y las empresas.

Con respecto a la seguridad no hay nada para agregar, solo prestar atención a los principios de seguridad informática. Esto no significa que cumpliendo estos principios un sistema informático va a ser invulnerable, pero estaríamos ayudando a que no ingresen hackers a los sistemas y que no nos envíen virus, porque como ya vimos, estos pueden ser letales para nuestras computadoras.
Como recomendación puedo sugerir la instalación de Linux (aunque esto significa incrementas los costos en lo que se refiere a capacitación), ya que se puede bajar de Internet (la pagina es www.linux.org). O bien la instalación de un excelente antivirus como es el "**Norton Antivirus Corporate Edition**".

ANEXO A. Superagentes, hackers y cuestiones de soberanía.
Clarín. 27-08-2002. Sociedad
La ley contra los delitos informáticos que está tratando el Congreso argentino está destinada a padecer los mismos obstáculos que enfrentan estas leyes en cualquier país. Porque no contempla una característica que hace a la naturaleza misma de Internet: su carácter supranacional. No hay una Internet argentina ni una Internet de Brasil ni de los Estados Unidos ni de Francia.
Internet es un **territorio no-geográfico** y toda ley sobre este territorio puede entrar en **conflicto con las soberanías** de los países. Si un ciudadano suizo, saudita o chino vulnera un sitio web alojado en la Argentina, ¿bajo la ley de qué país será juzgado?
En noviembre de 2000 el FBI logró capturar a dos ciudadanos rusos, Vasily Gorshkov, de 26 años, y Alexey Ivanov, de 20, acusados de haber violado la seguridad de al menos 40 empresas estadounidenses, realizar fraudes y robar tarjetas de crédito y datos personales con propósitos extorsivos.
Los agentes que participaron en la captura fueron premiados en los Estados Unidos por la brillante operación. Pero los rusos vieron la historia desde otro punto de vista. El 15 de agosto **el servicio de inteligencia ruso FSB acusó al agente del FBI Michael Schuler** de haber entrado sin autorización en servidores rusos para obtener la captura. Es decir, le reprochó exactamente **haber usado técnicas de hacking**, en lo que parece ser un novedoso capítulo de una serie de "superagentes".
Para combatir lo que técnicamente la ley de su propio país define como un delito informático, Schuler cometió otro delito informático. Paradójicamente, recibió del FBI **un premio a la excelencia** (por haber utilizado por primera vez en la historia del FBI la "técnica de captura extraterritorial" en un "cyber crimen"). Y del FSB recibió **una formal acusación**, enviada directamente al Departamento de Justicia de los Estados Unidos.
A Rusia no le gustó en lo más mínimo que husmearan en computadoras de su territorio y alegó **cuestiones de soberanía**. "Si los hackers rusos son sentenciados sobre la base de información obtenida por los Estados Unidos mediante el hacking, esto implicará la futura posibilidad de los servicios secretos estadounidenses de utilizar métodos ilegales en la recopilación de información en Rusia y otros países", dijo una fuente del FSB citada por la agencia de noticias **Interfax**.
Esto que parece un enfrentamiento en versión digital entre las agencias de ficción televisiva "Caos" y "Control" (aunque no se entienda quién es el malo y quién el bueno de la película) puede dar una idea de los problemas que se perfilan cuando se aplican **leyes nacionales** sobre Internet.
Hay otro aspecto ejemplificador en esta historia: ¿cómo realizaron sus intrusiones los dos jóvenes rusos? Generalmente, utilizando un reconocido agujero de seguridad del sistema operativo de Microsoft Windows NT, según reporta **Msnbc.com** (una fuente fuera de sospecha en este asunto, ya que pertenece a la propia Microsoft, en sociedad con la NBC).

De acuerdo con **Msnbc.com**, el "patch" (literalmente "parche") contra esa vulnerabilidad estuvo disponible en Internet durante casi dos años, pero los administradores de los sistemas violados "olvidaron" ponerlo. Podría suceder que algunas empresas prefieran hacer gastar dinero de los gobiernos (es decir, de todos nosotros) en la persecución de intrusos, en vez de gastar dinero propio en empleados que recuerden realizar la simple operación de instalar un archivo que corrige una falla de seguridad.

El fenómeno de la violación de los sistemas no es sólo un fenómeno de criminalidad (que, como tal, debe ser castigado). **Las empresas tienen una responsabilidad compartida**, y habría menos delitos informáticos si no les hicieran fácil la vida a los intrusos. Es decir, si se reflexionara sobre la importancia de la seguridad y se tomaran las previsiones pertinentes. Quien no pone una cerradura efectiva a la puerta de su casa (o a la puerta de su sistema, en este caso) está casi invitando a que le roben.
El problema esencial no es sólo definir un delito y su sanción, sino examinar **si la ley es eficaz y aplicable en la realidad internacional que plantea la naturaleza de Internet**.

ANEXO B. Un hacker saqueó las cuentas de 21 ahorristas.
Clarin.com 5-07-2002.
Un hacker chino logró introducirse en las computadoras de 21 clientes del Banco DBS de Singapur, y huyó hacia Malasia con 62.000 dólares singapurenses (u$s 37.000) luego de saquear las cuentas de los ahorristas sin necesidad de romper, ni trucar o manipular las defensas informáticas de la institución.
El individuo hackeó las máquinas de sus víctimas y obtuvo así sus códigos de usuario y contraseñas. Con estos datos pudo acceder a sus cuentas bancarias y retirar de cada una de ellas entre 200 y 4.999 dólares singapurenses, el máximo permitido.
Las autoridades del banco, que tiene 370.000 clientes a través de Internet, reintegraron el dinero a sus clientes, pero advirtieron que futuras estafas no serán reintegradas. Asimismo, instaron a sus clientes a mantener sus contraseñas en reserva, revisar regularmente sus cuentas, borrar las fichas de su historia como clientes, evitar guardar nombres de usuario y números PIN en sus computadoras e instalar la última versión de un programa antivirus.

FUENTES.
www.fbi.gov
www.delitosinformaticos.com
http://personales.ciudad.com.ar/roble/thaisdelitosinformaticos.htm
http://microasist.com.mx
http://edadfutura.metropoliglobal.com
http://www.rincondelvago.com/html/sotano/informatica/rincon_del_hacker/rincon_del_hacker.html
www.clarin.com.ar
http://www.solorecursos.com
http://www.conozcasupc.com.ar/
http://www.atlas-iap.es/~pepcardo/index.shtml?http://www.atlas-iap.es/~pepcardo/curs2.htm
http://www.linux.org/
Leer más: http://www.monografias.com/trabajos14/sisteinform/sisteinform2.shtml#ANEXO#ixzz2zAlzWRIh

TOMADO DE:

http://www.monografias.com/trabajos14/sisteinform/sisteinform.shtml