Seguridad informática

Autor: Jorge Saúl Sánchez Molina

Tesina presentada para obtener el título de:

Lic. En sistemas computarizados [sic]

Nombre del asesor:

Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA M.R.

FACULTAD DE SISTEMAS COMPUTARIZADOS

CLAVE 16PSU0014Q No. DE ACUERDO: 952006

" SEGURIDAD INFORMÁTICA "

TESINA

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN
SISTEMAS COMPUTARIZADOS

PRESENTA

JORGE SAÚL SÁNCHEZ MOLINA

ASESORES DE TESIS:

ING. Y M.A. SERGIO FRANCISCO BARRAZA IBARRA

MORELIA, MICH., ENERO 2004.

AGRADECIMIENTOS

Esta tesina es resultado del esfuerzo, trabajo y de la cooperación de muchas personas que hicieron posible la terminación de este proyecto.

Este proyecto es la culminación de un esfuerzo y no hubiera sido posible sin el apoyo del Ing. Sergio Francisco Barraza Ibarra, asesor de esta tesina que con su apoyo, sus consejos, opiniones y cometarios hicieron posible la culminación de esta tesina .Gracias

Gracias por todo el apoyo y cariño de mis padres José Alejandro Sánchez calzada y Rosalía Molina Vargas que sin ustedes no hubiera sido posible la realización de esta tesina, gracias por que siempre estuvieron en cada momento.

A mis hermanos por apoyarme y alentarme en situaciones difíciles.

A mis compañeros de clase, que siempre me apoyaron y me ayudaron a lo largo de mi carrera universitaria. Gracias

A mis amigos en general que siempre me estuvieron alentando para la realización de esta tesina.

Finalmente quiero agradecer a todos mis maestros por compartir sus conocimientos y por apoyarme, ayudarme a lo largo de mi carrera.

Introducción

A su vez la globalización de la información a través de Internet hace que los recursos informáticos se encuentren expuestos en mayor medida al ataque de terceros que produzcan tanto la caída de un servicio crítico como la pérdida o alteración de la información almacenada. Es por este motivo que cada día es más importante evaluar periódicamente los aspectos de seguridad tanto física como lógica, que permitan corregir las irregularidades y alcanzar el objetivo primordial de mantener las aplicaciones críticas de negocio estables, disponibles y protegidas en todo momento.

Uno de los cambios más sorprendentes del mundo de hoy en día es la rapidez de las comunicaciones. Modernos sistemas permiten que el flujo de información sea independiente del lugar físico donde nos encontremos. En ese sentido, ya no sorprende la transferencia de información en tiempo real o instantáneo y debido a que el conocimiento es poder; para adquirirlo, las empresas se han unido en grandes redes internacionales para transferir datos, sonidos e imágenes, y realizar el comercio en forma electrónica, con objeto de ser más eficientes. No obstante, al unirse en forma pública se han vuelto vulnerables, pues cada sistema de computadoras involucrado en la red es un blanco potencial y apetecible para obtener información.

El escenario electrónico actual en el cual las organizaciones enlazan sus redes internas a la Internet, crece a razón de más de un 10% mensual. Al unir una red a la Internet se tiene acceso también a las redes de otras organizaciones. De la misma forma en que accedemos a la oficina del frente de nuestra empresa, se puede recibir información de un servidor en Australia, conectarnos a una supercomputadora en Washington o revisar o buscar información de cualquier parte del mundo. Al haber de varias decenas de millones de computadoras interconectadas, no es difícil pensar que pueda haber más de una persona con perversas intenciones respecto de una organización. Por ello, es fundamental tener protegida adecuadamente la red.

Con mayor frecuencia se encuentran noticias sobre la violación de redes, servidores de importantes organizaciones por criminales informáticos desconocidos. A pesar de que la prensa ha destacado que tales intrusiones son solamente obra de adolescentes con propósitos de entretenerse o de jugar, ya no se trata de un incidente aislado de una desafortunada institución. De manera permanente se reciben reportes de los ataques a redes informáticas, los que se han vuelto cada vez más siniestros: los archivos son alterados subrepticiamente, las computadoras se vuelven inoperativas, se ha copiado información confidencial sin autorización, se ha reemplazado el software para agregar "puertas traseras" de entrada y miles de contraseñas han sido capturadas a usuarios inocentes; por mencionar algunas cuestiones.

Una vez conocida la realidad de los riesgos informáticos, es necesario desarrollar un "Plan de Seguridad Informática", el que en base en Medidas de prevención, Medidas de detección y Medidas de corrección que determine los controles o políticas que nos permiten mitigar el riesgo y llevarlo a un nivel aceptable. Para su desarrollo debe tenerse

siempre presente que los objetivos de seguridad informática es el resguardo de la confidencialidad, integridad y disponibilidad de los recursos de la información.

Objetivo de este trabajo

Dar a conocer la importancia que tiene la seguridad informática en una empresa, identificando las amenazas que pudiera sufrir la información, conocer los diferentes tipos de herramientas para proteger la información y hacer conciencia que toda organización necesita una estrategia de seguridad.

Definiciones

El concepto de seguridad se refiere a todo tipo de precauciones y protecciones que se llevan a cabo para evitar cualquier acción que comprometa a la información.

La seguridad informática es el nombre genérico dado a una colección de herramientas diseñadas para proteger datos y detener a los perpetradores, es decir, es la protección de los sistemas de cómputo para evitar amenazas de confidencialidad, integridad o disponibilidad.

El principio de la seguridad de la red es proteger el entorno de cualquier tipo de amenazas de seguridad mediante servicios de seguridad, mecanismos, y técnicas para hacer cumplir una política de seguridad.

La Seguridad Informática resguarda la información manejada por una computadora, y vela por que no sea dañada ni alterada por intrusos y esté disponible en cualquier momento, manteniéndose confidencial, en caso de ser necesario.

¿Por Qué Necesitamos Seguridad?

La información ha adquirido un elevado valor estratégico. El rápido avance de tecnologías informáticas nos ha hecho altamente dependientes de los sistemas automatizados de información que dan soporte a nuestras operaciones.

En antaño la seguridad no era un problema: la información se procesaba en centros de cómputo con una sola máquina y muy pocos terminales. El esquema de procesamiento estaba centralizado. Los terminales eran no inteligentes y había un único sistema operativo.

Las redes eran pequeñas y locales (pocos nodos y todos internos. Al no existir necesidad de seguridad no había razón para la misma.

La seguridad es un gran problema: los sistemas informáticos están dispersos en toda la organización. Se dispone de numerosas máquinas de distinto tipo. Se interconectan en red con las sucursales y con otras empresas. Tenemos redes de área amplia, Internet, diversidad de plataformas, múltiples sistemas operativos, usuarios internos, externos, invitados, computadoras personales, redes heterogéneas, computación móvil, virus, etc. Todo ello obliga a una mayor concienciación de la seguridad informática. Las normas corporativas, los entes reguladores y la competencia nos exigen tener seguridad.

Además cada día crecen los ataques de hackers y salen a la luz nuevas vulnerabilidades y virus en los sistemas informáticos.
Por ello es conveniente estar al día y anticiparse en caso de algún a tipo de ataque a nuestros sistemas de información.

¿Qué es la seguridad informática?

En realidad es un concepto cuya definición exacta es difícil de proporcionar, debido a la gran cantidad de factores que intervienen. Sin embargo es posible enunciar que Seguridad es el conjunto de recursos (metodologías, documentos, programas y dispositivos físicos) encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

Objetivos que persigue

Como ya se mencionaba en la introducción los objetivos que persigue la seguridad de los es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Incluyendo en esto los equipos, medios de almacenamiento, software, listados de impresora y los datos. Todo esto enmarcado en un objetivo que es el de mantener la **continuidad de los procesos** organizacionales que soportan los sistemas de información.

Propiedades de la Información que protege la Seguridad Informática

La seguridad informática es algo que ha ido adquiriendo cada vez más relevancia a medida que el uso de las redes de ordenadores se ha convertido en algo cada vez más mayoritario. Entre tanta gente conectada a la Red siempre surgen colectivos e individuos que atentan contra la integridad y la privacidad de los sistemas, ya sea por razones económicas o por puro reto intelectual. De cualquier forma, la amenaza es real y si nos interesa tener nuestros

contenidos a salvo tendremos que tomar medidas para evitar la intrusión en nuestros sistemas. En este capítulo detallaremos algunas reglas fundamentales que sirvan como base para conseguir un entorno seguro.

Cuando nos referimos a la expresión ``*seguridad informática*'' no estamos sólo comentando la forma de conseguir que alguien acceda a través de Internet o de cualquier forma a nuestro ordenador, sino que hablamos de un conjunto de actitudes y acciones destinadas a varias cosas:

- Garantizar la confidencialidad de nuestra información.
- Asegurar que nuestras conexiones no sean espiadas o atrapadas
- Que podamos estar seguros de que la información que tenemos no haya sido modificada.
- Conseguir que nuestra identidad no pueda ser falsificada y utilizada por otros.
- Evitar los problemas que conllevarían una pérdida de datos o incluso el borrado de nuestra información.
- Garantizar la autenticidad de los usuarios que acceden a la información.

Estos son algunos de los objetivos que pretendemos conseguir, para ello utilizaremos distintas herramientas y sobre todo deberemos tener una forma activa de enfocar el tema de la seguridad. Esto es algo muy importante, ya que la seguridad del sistema no es algo que se haga solo, necesita de nuestra supervisión.

La *seguridad informática* engloba los diferentes procedimientos y técnicas que garanticen los tres requisitos siguientes:

- **CONFIDENCIALIDAD**: Protege los Activos de Información contra accesos o divulgación no autorizados.
- **INTEGRIDAD**: Garantiza la exactitud de los Activos de Información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
- **DISPONIBILIDAD**: Asegura que los Recursos Informáticos y los Activos de Información pueden ser utilizados en la forma y tiempo requeridos. Bajo el punto de vista de Seguridad, la disponibilidad se refiere a su posible recuperación en caso de desastre y no al concepto de Nivel de Servicio empleado en otras áreas.

En esta tesina de **"La seguridad informática"** se hablara de:

Seguridad Física

Este capitulo implica mantener la integridad física de los equipos de computo, también tratara sobre los riegos tecnológicos, riesgos naturales y los riesgos humanos.

Protección de los datos(Seguridad Lógica)

Este capitulo implica mantener la integridad y consistencia de los datos. La principal función de la seguridad lógica es poner o aplicar herramientas de seguridad que protejan y resguarden el acceso a la información, permitiendo acceder a la información al personal autorizado.

Tipos De Ataques

Este capitulo tratara de los diversos tipos de ataques, de virus y sus diferentes clasificaciones, y todas aquellas acciones que supongan una violación de la seguridad de nuestro sistema.

Implementación De Políticas De Seguridad.

Este capitulo implica la implementación de las políticas de seguridad informática como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

SEGURIDAD FISICA

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de Dos, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural.

La seguridad física es una de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no.

La sala de la computadora deberá estar ubicada en una zona que no se exponga a riesgo de inundaciones y separada de las áreas adyacentes con paredes resistentes al fuego. Fuentes de energía interrumpidas, controladores y reguladores de las variaciones de la electricidad son también necesarias para procurar un procesamiento continuo y adecuado de los datos.

objetivo

Evitar riesgos potenciales de ataque, pérdida, robo o daño a los Sistemas de Información de la empresa, accidentales o intencionados, que puedan ocasionar la interrupción, total o parcial, de las actividades de negocio. En este capítulo se pretende definir los medios a utilizar para la protección de las instalaciones donde están situados los Recursos Informáticos, incluyendo cualquier tipo de soporte físico, que contienen los Activos de Información de la empresa.

Las Principales Amenazas Que Se Prevén En Seguridad Física Son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre
3. Disturbios, sabotajes internos y externos deliberados

Características De Construcción

Los edificios o instalaciones de una empresa donde están o estarán situados sus Sistemas de Información requieren unas características adicionales de protección física que deben ser consideradas antes de seleccionar su ubicación, teniendo en cuenta:

- La posibilidad de daños por fuego, inundación, explosión, disturbios civiles, amenazas de vecindad, cercanía de instalaciones peligrosas (depósitos de combustible, aeropuertos, acuartelamientos, etc.),
- Cualquier otra forma de desastre natural o provocado.
- Los elementos constructivos internos (puertas, paredes, suelos, etc.) deben cumplir el máximo nivel de protección.
- Estas instalaciones deben estar diseñadas de forma que no se faciliten indicaciones de su propósito ni se pueda identificar la localización de los Recursos informáticos.
- Deben incluir zonas destinadas a carga y descarga de suministros, y su inspección de seguridad. Si todos los materiales no pueden ser inspeccionados en el momento, debe habilitarse una zona de consigna o depósito de materiales transeúntes hasta que puedan ser revisados.
- Tienen que disponer de canalizaciones adecuadas para la conducción del cableado de comunicaciones y electricidad, para evitar ataques (sabotaje, fuego, roedores), interceptación o perturbaciones por fuentes de emisión próximas (radio, eléctricas, calor, etc.).
- Las áreas donde se encontraran los equipos más delicados deberán tener piso y techo falso.

Distribución De Áreas

El edificio o instalaciones de la empresa pueden estar distribuido en varias áreas o zonas que, dependiendo de su utilización y los bienes contenidos, tienen que estar sometidas a una serie de controles de acceso.
Pueden distribuirse las instalaciones de acuerdo con los criterios y denominaciones siguientes:
Áreas Públicas Espacios en los que no hay ningún tipo de restricción de acceso a empleados o personas ajenas a la empresa.
Áreas Internas Espacios reservados habitualmente a los empleados y personas ajenas a la empresa con autorización por motivos de negocio. Puede haber en ellos Recursos Informáticos, con un valor bajo.

1. Áreas de Acceso Limitado Espacios cuyo acceso está reservado a un grupo reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito.

Pueden concentrarse en ellos Recursos Informáticos que, en conjunto, tienen un valor medio.

2. Áreas de Acceso Restringido Espacios cuyo acceso está reservado a un grupo muy reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito, que tengan necesidad de acceder por razones de negocio.

   En ellos se concentran Recursos Informáticos que, en conjunto tienen un alto valor o contienen Activos de Información críticos para las actividades de negocio.

   A las dos últimas se les denomina Áreas Controladas.Tienen que permanecer cerradas, incluso cuando estén atendidas, y sus accesos controlados.

Áreas De Acceso Limitado

Cada una de las áreas de Acceso Limitado tiene que tener identificado formalmente un responsable o Propietario, cuyas responsabilidades serán:

Aprobar y mantener actualizada, una lista o relación de las personas con autorización de acceso permanente.

Aunque no se requiere una revisión periódica formal de la lista de acceso, las personas que tengan su autorización cancelada, por petición de su dirección o por haber causado baja en la empresa, tienen que ser eliminados de la relación de acceso en un tiempo razonable.

Aprobar accesos temporales a estas áreas. En este caso, la persona autorizada debe tener en cuenta que la autorización es para "una sola vez".

Áreas De Acceso Restringido

La entrada a estas áreas tiene que ser desde un área Interna o un área de Acceso Limitado, nunca desde un área Pública, y no deben tener ventanas al exterior.

Tiene que tener barreras de aislamiento de suelo a techo, incluyendo el falso suelo y el falso techo, o bien detectores volumétricos de intrusos.

Cada una de las áreas de Acceso Restringido tiene que tener identificado formalmente un responsable o Propietario, cuyas responsabilidades serán:

- Aprobar y mantener actualizada, una lista o relación de las personas con autorización de acceso permanente.

La lista de acceso debe ser actualizada siempre que haya cambios que así lo aconsejen y revisada formalmente, al menos, cada seis meses. Las personas que tengan su autorización cancelada, por petición de su dirección o por haber causado baja en la empresa, tienen que ser eliminados de la lista de acceso inmediatamente.

- Aprobar los accesos temporales a estas áreas, incluyendo los accesos del personal que, estando destinado en el área, accede fuera de su jornada laboral. En este caso, la persona autorizada debe tener en cuenta que la autorización es para "una sola vez". Las autorizaciones temporales deben contener:
  - nombre de quien autoriza, si no es el propietario,
  - el nombre del visitante autorizado,
  - razón social (sí corresponde) o motivo,
  - fecha y hora del acceso, y la firma,
  - fecha y hora de salida, y la firma,

El propósito de este registro es tener un archivo histórico de accesos, a utilizar en caso de investigación de incidente de Seguridad, pero en ningún caso es una herramienta de control de los empleados. El Propietario del área debe revisar, al menos mensualmente, que estos registros de acceso contienen la información descrita.

RIESGOS AMBIENTALES

Los riesgos ambientales es un problema que no suele ser tan habitual, pero que en caso de producirse pueden acarrear gravísimas consecuencias, es el derivado de los desastres naturales y su (falta de) prevención.

Inundaciones y humedad

Cierto grado de humedad es necesario para un correcto funcionamiento de nuestras máquinas: en ambientes extremadamente secos el nivel de electricidad estática es elevado, lo que, como veremos más tarde, puede transformar un pequeño contacto entre una persona y un circuito, o entre diferentes componentes de una máquina, en un daño irreparable al *hardware* y a la información. No obstante, niveles de humedad elevados son perjudiciales para los equipos porque pueden producir condensación en los circuitos integrados, lo que origina cortocircuitos que evidentemente tienen efectos negativos sobre cualquier elemento electrónico de una máquina.

Controlar el nivel de humedad en los entornos habituales es algo innecesario, ya que por norma nadie ubica estaciones en los lugares más húmedos o que presenten situaciones extremas; no obstante, ciertos equipos son especialmente sensibles a la humedad, por lo que es conveniente consultar los manuales de todos aquellos de los que tengamos dudas. Quizás sea necesario utilizar alarmas que se activan al detectar condiciones de muy poca o

demasiada humedad, especialmente en sistemas de alta disponibilidad o de altas prestaciones, donde un fallo en un componente puede ser crucial.

Cuando ya no se habla de una humedad más o menos elevada sino de completas inundaciones, los problemas generados son mucho mayores. Casi cualquier medio (una máquina, una cinta, un *router*...) que entre en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos.

Evidentemente, contra las inundaciones las medidas más efectivas son las de prevención (frente a las de detección); podemos utilizar detectores de agua en los suelos o falsos suelos de las salas de operaciones, y apagar automáticamente los sistemas en caso de que se activen. Tras apagar los sistemas podemos tener también instalado un sistema automático que corte la corriente: algo muy común es intentar sacar los equipos - previamente apagados o no - de una sala que se está empezando a inundar; esto, que a primera vista parece lo lógico, es el mayor error que se puede cometer si no hemos desconectado completamente el sistema eléctrico, ya que la mezcla de corriente y agua puede causar incluso la muerte a quien intente salvar equipos. Por muy caro que sea el *hardware* o por muy valiosa que sea la información a proteger, nunca serán magnitudes comparables a lo que supone la pérdida de vidas humanas. Otro error común relacionado con los detectores de agua es situar a los mismos a un nivel superior que a los propios equipos a salvaguardar (incluso en el techo, junto a los detectores de humo); evidentemente, cuando en estos casos el agua llega al detector poco se puede hacer ya por las máquinas o la información que contienen.

Medidas de protección menos sofisticadas pueden ser la instalación de un falso suelo por encima del suelo real, o simplemente tener la precaución de situar a los equipos con una cierta elevación respecto al suelo, pero sin llegar a situarlos muy altos por los problemas que ya hemos comentado al hablar de terremotos y vibraciones

Terremotos

Los terremotos son el desastre natural menos probable, por tanto, no se suelen tomar medidas serias contra los movimientos sísmicos, ya que la probabilidad de que sucedan es tan baja que no merece la pena invertir dinero para minimizar sus efectos.

De cualquier forma, aunque algunas medidas contra terremotos son excesivamente caras, no cuesta nada tomar ciertas medidas de prevención; por ejemplo, es muy recomendable no situar nunca equipos delicados en superficies muy elevadas (aunque tampoco es bueno situarlos a ras de suelo). Si lo hacemos, un pequeño temblor puede tirar desde una altura considerable un complejo *hardware*, lo que con toda probabilidad lo inutilizará; puede incluso ser conveniente (y barato) utilizar fijaciones para los elementos más críticos, como las CPUs, los monitores o los *routers*. De la misma forma, tampoco es recomendable situar

objetos pesados en superficies altas cercanas a los equipos, ya que si lo que cae son esos objetos también dañarán el hardware.

Para evitar males mayores ante un terremoto, también es muy importante no situar equipos cerca de las ventanas: si se produce un temblor pueden caer por ellas, y en ese caso la pérdida de datos o *hardware* pierde importancia frente a los posibles accidentes - incluso mortales - que puede causar una pieza voluminosa a las personas a las que les cae encima. Además, situando los equipos alejados de las ventanas estamos dificultando las acciones de un potencial ladrón que se descuelgue por la fachada hasta las ventanas, ya que si el equipo estuviera cerca no tendría más que alargar el brazo para llevárselo.

Vibraciones

Desde las más grandes (los terremotos) hasta las más pequeñas (un simple motor cercano a los equipos). Las vibraciones, incluso las más imperceptibles, pueden dañar seriamente cualquier elemento electrónico de nuestras máquinas, especialmente si se trata de vibraciones continuas: los primeros efectos pueden ser problemas con los cabezales de los discos duros o con los circuitos integrados que se dañan en las placas. Para hacer frente a pequeñas vibraciones podemos utilizar plataformas de goma donde situar a los equipos, de forma que la plataforma absorba la mayor parte de los movimientos; incluso sin llegar a esto, una regla común es evitar que entren en contacto equipos que poseen una electrónica delicada con *hardware* más mecánico, como las impresoras: estos dispositivos no paran de generar vibraciones cuando están en funcionamiento, por lo que situar una pequeña impresora encima de la CPU de una máquina es una mala idea.

Tormentas eléctricas

Las tormentas eléctricas son muy poco probables ya que hoy en día existen medidas de seguridad como para rayos que la mayoría de los edificios y casas cuentan con ellos, Si cayera un rayo sobre la estructura metálica del edificio donde están situados nuestros equipos es casi seguro que podemos ir pensando en comprar otros nuevos; sin llegar a ser tan dramáticos, la caída de un rayo en un lugar cercano puede inducir un campo magnético lo suficientemente intenso como para destruir *hardware* incluso protegido contra voltajes elevados.

Una medida de protección contra las tormentas eléctricas hace referencia a la ubicación de los medios magnéticos, especialmente las copias de seguridad; aunque hablaremos con más detalle de la protección de los *backups* se deben de almacenar lo más alejados posible de la estructura metálica de los edificios. Un rayo en el propio edificio, o en un lugar cercano, puede inducir un campo electromagnético lo suficientemente grande como para borrar de golpe todas nuestras cintas o discos, lo que añade a los problemas por daños en el *hardware* la pérdida de toda la información de nuestros sistemas.

Incendios y Humo

Una causa casi siempre relacionados con la electricidad son los incendios, y con ellos el humo; aunque la causa de un fuego puede ser un desastre natural, lo habitual en muchos entornos es que el mayor peligro de incendio provenga de problemas eléctricos por la sobrecarga de la red debido al gran número de aparatos conectados al tendido. Un simple cortocircuito o un equipo que se calienta demasiado pueden convertirse en la causa directa de un incendio en el edificio.

Un método efectivo contra los incendios son los extintores situados en el techo, que se activan automáticamente al detectar humo o calor. Algunos de ellos, los más antiguos, utilizaban agua para apagar las llamas, lo que provocaba que el *hardware* no llegara a sufrir los efectos del fuego si los extintores se activaban correctamente, pero que quedara destrozado por el agua expulsada. Visto este problema, a mitad de los ochenta se comenzaron a utilizar extintores de halón; este compuesto no conduce electricidad ni deja residuos, por lo que resulta ideal para no dañar los equipos. Sin embargo, también el halón presentaba problemas: por un lado, resulta excesivamente contaminante para la atmósfera, y por otro puede asfixiar a las personas a la vez que acaba con el fuego. Por eso se han sustituido los extintores de halón (aunque se siguen utilizando mucho hoy en día) por extintores de dióxido de carbono, menos contaminante y menos perjudicial. De cualquier forma, al igual que el halón el dióxido de carbono no es precisamente sano para los humanos, por lo que antes de activar el extintor es conveniente que todo el mundo abandone la sala; si se trata de sistemas de activación automática suelen avisar antes de expulsar su compuesto mediante un pitido.

RIESGOS TECNOLOGICOS.

Sobre cargas

Quizás los problemas derivados del entorno de trabajo más frecuentes son los relacionados con el sistema eléctrico que alimenta nuestros equipos; cortocircuitos, picos de tensión, cortes de flujo a diario amenazan la integridad tanto de nuestro *hardware* como de los datos que almacena o que circulan por él.

El problema menos común en las instalaciones modernas son las subidas de tensión, conocidas como `picos' porque generalmente duran muy poco: durante unas fracciones de segundo el voltaje que recibe un equipo sube hasta sobrepasar el límite aceptable que dicho equipo soporta. Lo normal es que estos picos apenas afecten al *hardware* o a los datos gracias a que en la mayoría de equipos hay instalados fusibles, elementos que se funden ante una subida de tensión y dejan de conducir la corriente, provocando que la máquina permanezca apagada. Disponga o no de fusibles el equipo a proteger (lo normal es que sí

los tenga) una medida efectiva y barata es utilizar tomas de tierra para asegurar aún más la integridad; estos mecanismos evitan los problemas de sobre tensión desviando el exceso de corriente hacia el suelo de una sala o edificio, o simplemente hacia cualquier lugar con voltaje nulo. Una toma de tierra sencilla puede consistir en un buen conductor conectado a los chasis de los equipos a proteger y a una barra maciza, también conductora, que se introduce lo más posible en el suelo; el coste de la instalación es pequeño, especialmente si lo comparamos con las pérdidas que supondría un incendio que afecte a todos o a una parte de nuestros equipos.

Incluso teniendo un sistema protegido con los métodos anteriores, si la subida de tensión dura demasiado, o si es demasiado rápida, podemos sufrir daños en los equipos; existen acondicionadores de tensión comerciales que protegen de los picos hasta en los casos más extremos, y que también se utilizan como filtros para ruido eléctrico. Aunque en la mayoría de situaciones no es necesario su uso, si nuestra organización tiene problemas por el voltaje excesivo quizás sea conveniente instalar alguno de estos aparatos.

Interrupciones Eléctricas

Otro problema, muchísimo más habituales que los anteriores en redes eléctricas modernas, son los cortes en el fluido eléctrico que llega a nuestros equipos. Aunque un simple corte de corriente no suele afectar al *hardware*, lo más peligroso (y que sucede en muchas ocasiones) son las idas y venidas rápidas de la corriente; en esta situación, aparte de perder datos, nuestras máquinas pueden sufrir daños.

La forma más efectiva de proteger nuestros equipos contra estos problemas de la corriente eléctrica es utilizar un no break conectada al elemento que queremos proteger. Estos dispositivos mantienen un flujo de corriente correcto y estable de corriente, protegiendo así los equipos de subidas, cortes y bajadas de tensión; tienen capacidad para seguir alimentando las máquinas incluso en caso de que no reciban electricidad (evidentemente no las alimentan de forma indefinida, sino durante un cierto tiempo.

Un último problema es la corriente estática, un fenómeno extraño del que la mayoría de gente piensa que no afecta a los equipos, sólo a otras personas. Nada más lejos de la realidad: simplemente tocar con la mano la parte metálica de teclado o un conductor de una placa puede destruir un equipo completamente. Se trata de corriente de muy poca intensidad pero un altísimo voltaje, por lo que aunque la persona no sufra ningún daño - sólo un pequeño calambrazo - el ordenador sufre una descarga que puede ser suficiente para destrozar todos sus componentes, desde el disco duro hasta la memoria RAM. Contra el problema de la corriente estática existen muchas y muy baratas soluciones: *spray* antiestático, ionizadores antiestáticos. No obstante en la mayoría de situaciones sólo hace falta un poco de sentido común del usuario para evitar accidentes: No tocar directamente ninguna parte metálica, protegerse si debe hacer operaciones con el *hardware*, no mantener el entorno excesivamente seco.

Aire Acondicionado

Los ordenadores mientras están en funcionamiento, generar calor que desprenden de sí mismos a través de uno o más ventiladores. Esto hace que la sala donde se encuentren situados, por el efecto de uno o más ordenadores, vaya poco a poco calentándose. Además las altas temperaturas son contraproducentes para los ordenadores, llegando (algunos de ellos) a apagarse automáticamente si detectan que en la sala hay un exceso de temperatura.

Para evitar eso, en la sala de ordenadores, se deben de colocar equipos de aire acondicionado que bajen la temperatura hasta los márgenes adecuados para el correcto funcionamiento de los ordenadores.
Estos equipos se deben revisar y tener en mantenimiento para evitar que la avería del equipo haga que dejen de funcionar, e incluso, se estropeen los equipos.

Otra condición básica para el correcto funcionamiento de cualquier equipo que éste se encuentre correctamente ventilado, sin elementos que obstruyan los ventiladores de la CPU. La organización física del computador también es decisiva para evitar sobrecalentamientos: si los discos duros, elementos que pueden alcanzar temperaturas considerables, se encuentran excesivamente cerca de la memoria RAM, es muy probable que los módulos acaben quemándose.

Cableado

Como sabemos el cableado es la columna vertebral de la red de cualquier centro de computo lo cual debe tener mucho cuidado en la instalación para protegerlos de la humedad, agua, de los roedores o que estén al paso del personal, porque un cable dañado puede producir perdida de información y perdida de velocidad.
El cableado de cualquier centro de computo debe ser estructurado, estar protegido con canaletas, en lugares secos y ocultos.

AMENAZAS HUMANAS (amenazas a la información).

Robo.

Los equipos de cómputo son posesiones muy valiosas de las empresas y están expuestas al "robo", de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los operadores utilicen el computador de la empresa en realizar trabajos privados para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada. Muchas empresa invierten millones de dólares en programas y archivos de información, a los que dan menor

protección que la que otorgan a una máquina de escribir o una calculadora. El software, es una propiedad muy fácilmente sustraída, cintas y discos son fácilmente copiados sin dejar ningún rastro.

Fraude

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas en dicho propósito
En realidad, el potencial de pérdida a través de fraudes, y los problemas de prevención y detección del fraude, están en aumento en sistemas computarizados.
Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.
Las tres principales áreas donde se produce el fraude son:

1. Manipulación de información de entrada, fácil de realizar y muy difícil de detectar, al ser los métodos de validación de entrada simples y, en general, conocidos por un gran número de personas de la empresa.

2. Alteración o creación de archivos de información. Se alteran los datos directamente del fichero o se modifica algún programa para que realice la operación deseada.

3. Transmisión ilegal. Interceptar o transferir información de teleproceso.

Sabotaje

El peligro más temido por los centros de Computo, es el sabotaje. Empresas que han intentado implementar programas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros. Este puede ser un empleado o un sujeto ajeno a la propia empresa.

Los imanes son herramientas muy recurridas, aunque las cintas estén almacenadas en el interior de su funda de protección, una ligera pasada y la información desaparecerá. Una habitación llena de cintas puede ser destruida en pocos minutos. Los Centros de Procesamiento de Datos pueden ser destruidos sin entrar en ellos. Suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado. Las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

Destrucción

Sin las adecuadas medidas de seguridad las empresas pueden estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático. La destrucción del equipo puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, vandalismo, etc.

Para evitar daños mayores al ser destruida la información, debe hacerse **backups** de la información vital para la empresa y almacenarse en lugares adecuadamente preparados para ese fin y de preferencia aparte del local donde se encuentran los equipos que usualmente lo manejan.

Hay que protegerse también ante una posible destrucción del hardware o software por parte de personal no honrado. Por ejemplo: hay casos en los que, empleados que han sido recientemente despedidos o están enterados que ellos van a ser despedidos, han destruido o modificado archivos para su beneficio inmediato o futuro.

Modificación

La importancia de los datos que se modifican de forma ilícita, está condicionada al grado en que la organización depende de los datos para su funcionamiento y toma de decisiones. Si fuera posible, esto podría disminuir su efecto si los datos procedentes de las computadoras que forman la base de la toma de decisiones, se verificarán antes de decidir. Hay que estar prevenido frente a la tendencia a asumir que "si viene de la computadora, debe ser correcto".
Adicionalmente a proteger sus programas de Aplicación como activos, es a menudo necesario establecer controles rígidos sobre las modificaciones a los programas, para estar seguros de que los cambios no causan daños accidentales o intencionados a los datos o a su uso no autorizado.
Deben ser considerados como medidas de seguridad para proteger los datos en el sistema, las limitaciones en el ámbito de los programas de aplicación, auditorias y pruebas, revisiones de modificaciones, exclusión cuando sea necesario de los programas de aplicación de las áreas de sistemas (pase a la "Área de Producción" o a "Biblioteca de Programas") y restricciones efectivas en los programas de aplicación de las áreas de sistemas (necesidad de documento de autorización.)
Las empresas deben tener muy en cuenta los siguientes puntos para la protección de sus datos de una posible contingencia.
1. Hacer de la copia de seguridad una política, no una opción.

2 . Hacer que la copia de seguridad resulte deseable.

3 . Facilitar la ejecución de la copia de seguridad (equipos adecuados, disponibilidad, suministros).

4. Hacer la copia de seguridad obligatoria.

5 . Asegurarse de que los usuarios cumplen la política de copias de seguridad (Política de Auditoria a las Copias de Seguridad).

Una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad. Ejemplos de este ataque son el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

Vandalismo

Dentro de este apartado se engloban la mayoría de los "percances" que sufren los equipos informáticos educativos. Son muy comunes y su frecuencia aumenta a medida que ascendemos en la etapa educativa.

Los actos de vandalismo pueden dirigirse a cualquier parte de los equipos informáticos, sin embargo, en general, suelen centrarse en dos puntos esenciales: la unidad central y el sistema de red.

La unidad central es el sistema más vulnerable y las acciones suelen dirigirse a inutilizarla total o parcialmente.

La inutilización total suele basarse en la destrucción de la placa base o la fuente de alimentación. Preferiblemente esta última ya que destruyendo la fuente (por cortocircuito) se destruye también la placa base.

La inutilización parcial consiste en destruir o eliminar partes de la unidad central (interruptores, conectores, etc.) o elementos accesorios (teclado, ratón, etc.).

Chantaje

Otro problema que enfrentan las empresas por parte de sus empleados o ex empleados es el del chantaje el cual
Consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

Mascarada (masquerading)

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.

Interrupción.

Un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad. Ejemplos de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

Intercepción.

Una persona no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad. La entidad no autorizada podría ser una persona, un programa o un ordenador. Ejemplos de este ataque son pinchar una línea para hacerse con datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos), o bien la lectura de las cabeceras de paquetes para desvelar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).

Hackers

El hacker es aquél que entra ilegalmente a los sistemas, **roba información y provoca caos en sistemas** remotos. ¿Porqué lo hace?; bueno, hay varias respuestas, por diversión, por venganza, por pertenecer, o por sentir la adrenalina corriendo por sus venas. La forma más común en la que se encuentran en la red es presentando software y documentos para *atacar*. Estos ataques pueden ser entradas ilegales, adquisición de passwords de sistemas, y adquisición de software, siendo los juegos los blancos preferidos. También es común que entren a nuestra computadora para ver qué hacemos, qué tenemos, etc., este truco es muy usado por sitios que venden direcciones de e-mail y, por medio de *cookies* (galletas), reciben información del usuario, su sistema operativo, sus preferencias, su visualizador, etc. Las cookies son pequeños programas que envía un servidor para saber quién está en su sistema.

Crackers

Podría definirse como la persona que aplica sus vastos conocimiento de programación e informática para eliminar la seguridad de programas, juegos... En realidad los crackers suelen estar organizados en grupos en los que cada persona tiene encargada una función

muy concreta dentro de la creación de una crack (dícese del parche o programa auxiliar que evita la seguridad de un programa informático modificando a este o al sistema).

PERSONAL INTERNO

Ex Empleados

Son personas que no están conforme con su despido de la empresa o que han pasado a formar parte de otra empresa y buscan sacarle el mayor provecho de forma ilícita a los conocimientos y información adquiridos en la otra empresa como: robo, chantaje, sabotaje, etc.

Usuarios Incómodos

Personal que siente celos o incomodo con algún compañero o que no este conforme con su trabajo y busca causar un daño a la empresa o un beneficio propio. Ejemplo de algunos posibles daños: sabotaje, robo, modificación, etc.

CONTROL DE ACCESO FISICO AL PERSONAL.

Es necesario tener seguridad física para garantizar la seguridad global de los sistemas de información ya que si algún intruso puede llegar con facilidad al área donde se encuentran los equipos puede llegar a robar un disco duro, apagar los equipos de computo sabotear información o a modificarla.

El acceso físico a las áreas mencionadas sólo se le permitirá al personal autorizado por la gerencia. Todas las personas que requieran acceso a las áreas indicadas lo harán bajo un control adecuado y acompañados del supervisor o funcionario autorizado del área de operación

Prevención

Para prevenir un acceso físico no autorizado existen soluciones desde las más simples hasta las mas sofisticadas como analizadores de retina hasta videocámaras, pasando por tarjetas inteligentes o control de las llaves que abren determinada puerta.
Los más adecuados para la seguridad física sean los biométricos pero suelen resultar algo caros para utilizarlos masivamente en entornos de seguridad media.
Pero no hay que irse a sistemas tan complejos para prevenir accesos físicos no autorizados; normas tan elementales como cerrar las puertas con llave al salir de un laboratorio o un

despacho o bloquear las tomas de red que no se suelan utilizar y que estén situadas en lugares apartados son en ocasiones más que suficientes para prevenir ataques

Detección

Para la detección de accesos físicos no autorizados intervienen medios técnicos, como cámaras de vigilancia de circuito cerrado o alarmas.
Es importante si un usuario autorizado detecta presencia de alguien de quien sospecha que no tiene autorización para estar en una determinada área debe avisar inmediatamente al administrador o al responsable de los equipos, que a su vez puede avisar al servicio de seguridad si es necesario

Guardias

Los guardias son indispensables para la protección de la información de la empresa ya que ellos controlan y vigilan el acceso a las diferentes áreas.

Medios Técnicos de protección

TV. Circuito Cerrado

Es una herramienta de prevención básica en las areas de acceso restringido el cual nos permitirá vigilar y monitorear al personal que labore en esa área y también en caso de algún intruso poderlo detectar

Alarmas
Son dispositivos de prevención la cual se activara si se violan los sistemas de seguridad como ejemplo la forjadura de una puerta, ventana.

Sensor De Movimientos

Es un dispositivo de detección que se activa si hay algún movimiento en el área restringida el cual ayuda a detectar la presencia de algún intruso no autorizado.

SISTEMAS BIOMETRICOS

Con el avance de la tecnología se han diseñado dispositivos para proteger a un área determinada estos sistemas son los denominados **biométricos.**

Es ideal para aplicaciones que requieren única, absoluta y segura identificación del usuario. La información capturada es veraz, ya que la característica principal de los equipos es que identifican un rasgo físico del usuario, lo que hace imposible la suplantación o registro fraudulento. Los sistemas biométricos existentes son: Lectura de iris, Reconocimiento de voz, Lectura de huella digital, Reconocimiento de mano.

Huella Digital

La huella dactilar de una persona es un patrón permite determinar su identidad de forma segura ya que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.

Cuando un usuario quiera autenticarse ante el sistema sitúa su dedo en un área determinada (área de lectura, no se necesita en ningún momento una impresión en tinta). Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las minucias (ciertos arcos, bucles o remolinos de la huella) que va a comparar contra las que tiene en su base de datos; es importante resaltar que lo que el sistema es capaz de analizar no es la huella en sí sino que son estas minucias, concretamente la posición relativa de cada una de ellas. Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos 30 o 40 de Sí la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, y en caso contrario se le niega el acceso.

Una desventaja de este sistema es la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer (un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema). También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas

Verificación De Voz

En los sistemas de reconocimiento de voz no se intenta, como mucha gente piensa, reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de

forma que el reconocedor lo entienda y lo autentifique. Estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va `proponiendo' a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales...). Conforme va hablando el usuario, el sistema registra toda la información que le es útil; cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos.

Una desventaja de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir sí el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía su timbre...). A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios, siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

Verificación de patrones oculares

Los modelos de autenticación biométrica basados en patrones oculares se dividen en dos tecnologías diferentes: o bien analizan patrones retínales, o bien analizan el iris. Estos métodos se suelen considerar los más efectivos.

Retina

En los sistemas de autenticación basados en patrones retínales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanda la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

Iris

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo.

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retínales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado; esta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 *KBytes*) suficiente para los propósitos de autenticación. Esa muestra, denominada *iriscode* es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos

Geometría De La Mano

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura, Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.
Uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la mano (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autentificadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones: no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

PROTECCION DE DATOS (seguridad lógica)

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por él almacenada y procesada. Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

La principal función de la seguridad lógica es poner o aplicar herramientas de seguridad que protejan y resguarden el acceso a la información, permitiendo acceder a la información al personal autorizado.

La integridad y seguridad de los datos están estrechamente relacionadas por su propósito de proteger los datos de peligros potenciales. En el caso de la integridad de los datos el peligro es, a menudo, un simple error de cálculo, confusiones o errores cometidos por Personas, o fallos de equipos que provocan la pérdida de datos, su corrupción o su incorrecta modificación. En relación con la seguridad, la gente puede tratar de infiltrarse de forma intencionada en los sistemas de otras compañías para robar o estropear información en su propio beneficio.

Objetivos

Es mantener los datos y la información en un estado completo e inalterado. Esto significa que los datos no podrán ser modificados o perdidos por hechos accidentales o intencionados. Una pérdida de la integridad de los datos significa que ha pasado algo cuyo resultado ha sido su pérdida o modificación.

Proteger los Activos de Información de la empresa para que sean siempre utilizados de forma autorizada, y sólo por razones de negocio, y evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizados, de forma accidental o intencionada.

CONTROL DE ACCESO

Identificación De Usuario

Aprobar el uso de cada Sistema y conocer a sus usuarios, asegurando que cada identificador de usuario es único y sólo puede ser asociado a una persona.

Es la clave que permite a un usuario acceder de forma individual a un Sistema de Información. Cada identificador de usuario tiene que estar asignado a una persona, que será responsable de las actividades realizadas con él.

Generalmente, un identificador de usuario (junto con la contraseña o cualquier otro método de autenticación) se asigna a una persona para facilitarle el acceso a un único Sistema de Información, debiendo adquirir otros identificadores para el uso de otros Sistemas. Esto provoca la multiplicidad de identificadores y contraseñas, tanto más cuanto mayor sea el número de Sistemas existentes en la empresa y la necesidad de su utilización. Para resolver este posible problema, es recomendable:

- Definir y utilizar una nomenclatura estándar en la creación de identificadores, de forma que un usuario tenga el mismo identificador en todos los Sistemas que necesite utilizar;
- Instalar un Sistema de Control de Accesos capaz de gestionar más de un Sistema de Información, con lo que el identificador de usuario (y la contraseña asociada) serían únicos y válidos para todos los Sistemas;
- Utilizar un método de Identificación única, que permita al usuario realizar los procesos de identificación y autenticación una sola vez, en la primera conexión al sistema, pudiendo acceder posteriormente a cualquier otro Sistema o servicio por propagación o conversión a los distintos identificador de usuario y contraseña necesarios.

Adicionalmente, y dada la creciente necesidad de identificación (y autenticación) descritas, es posible dedicar un Sistema a las funciones de control de Seguridad, de modo que antes de permitir el acceso del usuario a cualquier Sistema de Información, se verifique una sola vez su identidad y autorizaciones de acceso. Este Sistema tendría que ser gestionado por el Administrador de Seguridad.

Autenticación De Usuarios

Asegurar que un usuario es quien dice ser, cuando accede al Sistema, En general, el proceso de autenticación de un usuario está basado en:

- Algo que sabe (contraseña);
- Algo que tiene (tarjeta, dispositivo, etc.);
- Algo que es (características biométricas).

La utilización de sólo uno de los métodos anteriores se denomina Autenticación Simple.

Cuando los controles de acceso tienen que ser especialmente restrictivos, pueden combinarse dos, o más, métodos para eliminar, o al menos reducir, los riesgos de

utilización no autorizada de un identificador de usuario. En este caso la denominación es Autenticación Reforzada.

La mayoría de los Sistemas de Información utilizan la Autenticación Simple por contraseña (password).

Contraseñas (Passwords)

La contraseña de acceso es, hoy por hoy, la principal protección porque verifica inequívocamente la identidad del usuario de un Sistema.

Deben considerarse información clasificada las contraseñas, o cualquier otro método utilizado, de autenticación de usuario de acuerdo con el máximo nivel de información clasificada que el usuario pueda utilizar en el Sistema.

Para la protección de los Activos de Información de la empresa y la protección del propio usuario, la contraseña:

- tiene que ser secreta y no compartida con nadie,
- no puede ser visualizada en pantalla mientras se teclea, y
- No puede ser almacenada en claro (sin cifrar), en ningún tipo de Activo de Información.

Los sistemas operativos que incluyen algún Sistema de Control de Accesos, llevan rutinas de verificación de la calidad de la contraseña para evitar que pueda ser trivial o predecible. En cualquier caso, la contraseña debe disponer, como mínimo, de las características de calidad siguientes:

- Tener una longitud mínima de 6 caracteres; o tener al menos un carácter numérico y uno alfabético;
- No empezar ni terminar con un número; o no tener mas de tres caracteres consecutivos idénticos, en cualquier posición, a los de una contraseña usada anteriormente;
- No tener mas de dos caracteres iguales consecutivos;
- Ser cambiada, al menos, cada 60 días para usuarios generales y cada 30 días para usuarios que tengan algún tipo de privilegio o autoridad. Tiene que haber instalado un control que informe a los usuarios cuando su contraseña tiene que ser cambiada;
- No ser reutilizada hasta después de, al menos, 12 cambios;
- No contener el identificador de usuario, como parte de la contraseña.

En muchos casos, sistemas operativos, productos informáticos o aplicaciones traen una contraseña 'por defecto' para ser usada durante su instalación. Sin excepción, estas

contraseñas tienen que ser cambiadas, si técnicamente es posible, durante la primera utilización o a la mayor brevedad posible, en caso contrario.

Si, por razones de negocio, una persona tiene que utilizar sistemas ajenos a la empresa, no debe utilizar en ellos la misma contraseña utilizada en los sistemas internos de la empresa.

Si el nivel de Seguridad es inferior en aquellos, podría ser detectada y utilizada sin autorización en los sistemas de la empresa.

Roles

El acceso a la información también se controla por roles o funciones del usuario que esta asignado previamente a dicho acceso como: programador, líder de proyectos, gerente, cajero y administrador de sistemas que es el que tiene le mayor grado de privilegios.

Privilegios Del Usuario

Los usuarios contaran con diferentes niveles de privilegios según el cargo del usuario será el acceso sobre los recursos y la información.

- **Lectura**: el usuario puede únicamente leer o visualizar la información pero no puede alterarla.
- **Escritura:** el usuario puede agregar datos, modificar y borrar información.
- **Ejecución:** este acceso le permite al usuario ejecutar y instalar programas.
- **Borrado:** permite al usuario eliminar recursos del sistema (programas, archivos, etc.)
- **Modificación:** le permite al usuario modificar la información.

CONTROL INTERNO

Respaldos

Las copias de seguridad son uno de los elementos más importantes y que requieren mayor atención a la hora de definir las medidas de seguridad del sistema de información ya que la información es vital para el funcionamiento de la empresa.

Soporte Utilizado

Es la primera decisión a tomar cuando se planea una estrategia de copia de seguridad, sin embargo esta decisión estará condicionada por un conjunto de variables, tales como la frecuencia de realización, el volumen de datos a copiar, la disponibilidad de la copia, el tiempo de recuperación del sistema, etc.

Entre los soportes más habituales, podemos destacar las cintas magnéticas, discos compactos (como las unidades de Iomega Zip y Jazz), grabadoras de CD-ROM o cualquier dispositivo capaz de almacenar los datos que se pretenden salvaguardar.

Frecuencia De Realización De Copias De Seguridad

La realización de copias de seguridad ha de realizarse diariamente, éste es el principio que debe regir la planificación de las copias, sin embargo, existen condicionantes, tales como la frecuencia de actualización de los datos, el volumen de datos modificados, etc., que pueden hacer que las copias se realicen cada más tiempo.

Planificación De La Copia

Las copias de seguridad se pueden realizar en diferentes momentos día, incluso en diferentes días, pero siempre se han de realizar de acuerdo a un criterio, y este nunca puede ser "cuando el responsable le recuerda", si es posible, la copia se debe realizar de forma automática por un programa de copia, y según la configuración de éste, se podrá realizar un día concreto, diariamente, semanalmente, mensualmente, a una hora concreta, cuando el sistema esté inactivo.

Mecanismos De Comprobación

Se deben definir mecanismos de comprobación de las copias de seguridad, aunque los propios programas que las efectúan suelen disponer de ellos para verificar el estado de la copia, es conveniente planificar dentro de las tareas de seguridad la restauración de una parte de la copia o de la copia completa periódicamente, como mecanismo de prueba y garantía.

Responsable Del Proceso

La mejor forma de controlar los procesos que se desarrollan en el sistema de información, aunque estos estén desarrollados en una parte importante por el propio sistema, es que exista un responsable de la supervisión de que " lo seguro es seguro", para ello se debe designar a una persona que incluya entre sus funciones la supervisión del proceso de copias de seguridad, el almacenamiento de los soportes empleados en un lugar designado a tal fin e incluso de la verificación de que las copias se han realizado correctamente.

También se recomienda guardar las copias de seguridad en un lugar alejado, como, por ejemplo, una caja de seguridad o cualquier otro sitio asegurado contra incendios, para que, en caso de que se produzca algún desastre como un incendio, los datos se encuentren protegidos.

Encriptación (criptografia)

Historia de la criptologia

La criptografía es tan antigua como la escritura. El arte de escribir en clave o en forma enigmática ha estado siempre presente. Sobre todo en épocas de guerra, donde la necesidad de que los mensajes no cayeran en manos enemigas era prioritaria.

Las civilizaciones más antiguas contaban con diferentes métodos para proteger sus comunicaciones. Mesopotamia, India y China usaban sus métodos de encriptación. Pero sin duda las referencias más conocidas son la egipcia, a través de los jeroglíficos, y la griega.

En Grecia, en el año 500 a.C., se usaba un artilugio llamado "Scytale". Se trataba de un cilindro alrededor del que se enrollaba una tira de cuero. Lo que se hacía era escribir sobre la piel el mensaje y al desenrollarlo aparecía una lista de letras sin sentido. De tal manera, que para leer el mensaje había que enrollar nuevamente el cuero sobre un cilindro de idéntico diámetro.

No obstante, a quien los expertos atribuyen el primer sistema de cifrado, tal y como los conocemos hoy en día, es a Julio César durante el Imperio Romano. Su método consistía en sustituir cada letra de un mensaje por la situada tres posiciones por delante en el alfabeto. Así, por ejemplo, si hay una A en realidad sería una D, y así con todas. Nadie logró descifrar ninguno de sus mensajes.

Durante la Edad Media, algunos copistas escondían sus nombres en los manuscritos, sustituyendo las vocales por puntos o consonantes arbitrarias.
Más tarde, los sistemas fueron evolucionando a partir del de Julio César y se pasó a elegir una reordenación cualquiera del alfabeto. Se hacía corresponder una letra con otra sin ningún patrón determinado. Roger Bacón en el siglo XII y León Batista Alberti en el siglo XV inventaron y publicaron sus respectivos algoritmos (conjunto de procesos matemáticos) de encriptación basados en el método de Julio César.

Ya en el siglo XX, con motivo de las dos guerra mundiales, la criptografía y sus técnicas

estaban a la orden del día. En la primera gran guerra el uso de estos métodos no fue muy exitoso, lo que hizo que ya en la segunda Guerra Mundial se desarrollaran las primeras técnicas electromagnéticas. Muestra de ello es Enigma, una máquina que usaban los alemanes para cifrar y descifrar sus mensajes. Un grupo de científicos del bando aliado se dedicaban a estudiarla, hasta que uno de ellos, Alan Turing, logró descifrar el primer mensaje de Enigma.

Hoy en día, con el avance de la tecnología y con la aparición de Internet en escena han proliferado y se han complicado las técnicas criptográficas. El comercio electrónico, los e-mails y las operaciones bancarias necesitan de métodos seguros que protejan la información que se maneja y a los usuarios. Por todo esto la criptografía es hoy y será en un futuro no muy lejano algo fundamental.

¿Qué Es La Criptografía?

La criptografía es la ciencia de usar las matemáticas para encriptar y desencriptar datos. Una vez que la información ha sido encriptada, puede ser almacenada en un medio inseguro o enviada a través de una red insegura (como Internet) y aún así permanecer secreta. Luego, los datos pueden desencriptarse a su formato original.

Criptografía Simétrica De Clave Secreta

Se basa en que emplea la misma clave para encriptar que para desencriptar, y entonces se habla de algoritmo de cifrado simétrico. La clave debe ser conocida tanto por el emisor como el receptor del mensaje y ambos deben mantenerla en estricto secreto, ya que si se conoce peligraría el contenido del mensaje.

Este tipo de cifrado ha dominado hasta hace un par de décadas. Los métodos criptográficos clásicos, como el de Julio César, pueden considerarse simétricos y los principales algoritmos simétricos actuales son DES, IDEA, RC5 y el novedoso AES.

Transposición, sustitución y producto

Se puede hacer otra gran división de los cifrados según el tipo de operación que se realiza en el cifrado. Dadas la característica finita del alfabeto y la hipótesis de no variación de la longitud del texto, existen dos opciones para el cifrado. La primera, llamada transposición, consiste en crear el texto cifrado simplemente desordenando las unidades que forman el texto original. La segunda, llamada sustitución, consiste en sustituir las unidades del texto original por otras.

El cifrado por transposición consiste en la alteración del orden de las unidades del texto original según una clave. El cifrado por sustitución consiste en el reemplazamiento de las unidades del texto original según una clave.

Se llama cifrado producto a la aplicación iterativa de cifrados sobre textos ya cifrados, es decir, a la composición de varios cifrados. En general, los cifrados simétricos son cifrados producto de las dos operaciones mencionadas, sustitución y transposición.

Sustitución y transposición no resultan muy efectivos usados individualmente, sin embargo constituyen la base de sistemas mucho más difíciles de criptoanalizar. Algunos de estos esquemas fueron usados en los años veinte para el diseño de las máquinas de rotor.

Cifrado en bloque, DES

Independientemente de la clasificación realizada en el apartado anterior según la fuente que genera el texto, los cifrados simétricos se pueden clasificar en dos grandes grupos: los correspondientes a fuentes que generan n-palabras y los correspondientes a fuentes que generan letras. En el primer caso se habla de cifrados en bloque y en el segundo de cifrados en flujo.
El cifrado en bloque opera sobre textos formados por n-palabras, convirtiendo cada una de ellas en una nueva n-palabra.

Sin duda el cifrado en bloque más conocido es el llamado DES. Este sistema se puede catalogar como un cifrado en bloque que es a la vez un cifrado producto de transposiciones y sustituciones.

A finales de los años cuarenta, Shannnon sugirió nuevas ideas para futuros sistemas de cifrado. Sus sugerencias se referían al uso de operaciones múltiples que mezclaran transposiciones y sustituciones. Estas ideas fueron aprovechadas por IBM en los años setenta, cuando desarrolló un nuevo sistema llamado LUCIFER. Poco después en 1976, el gobierno de EEUU adoptó como estándar un sistema de cifrado basado en el LUCIFER y denominado DES (Data Encryption Standard). En consecuencia casi todos los gobiernos del mundo aceptaron el mismo cifrado o parte de él como estándar en las comunicaciones de las redes bancarias y comerciales.

En el DES, el bloque de entrada M en primer lugar sufre una transposición bajo una permutación denominado IP, originando To=IP(M). Después de pasar To dieciséis veces por una función f, se transpone bajo la permutación inversa IP', obteniéndose así el resultado final.

Criptografía Asimétrica O De Llave Pública

La criptografía de clave o llave pública se basa en que emplea dos llaves diferentes: una para el cifrado (clave pública) y otra para el descifrado (clave privada).

La clave pública está a disposición de todo el mundo en Internet y la privada sólo la conoce su propietario. Estas llaves son una secuencia bastante compleja de caracteres y de números.

Otra utilidad de este sistema es que proporciona autentificación para mensajes. La clave privada del remitente puede emplearse para encriptar un mensaje firmándolo. Entonces se genera una firma digital, que el destinatario o cualquier otra persona puede comprobar al descifrarla con la clave pública del remitente. Así se demuestra el origen del mensaje y que no ha sido alterado por nadie. No es posible falsificar un texto firmado.

Sistemas basados en curvas elípticas.

En 1985, la teoría de las curvas elípticas encontró de la mano de Miller aplicación en la criptografía. La razón fundamental que lo motivó fue que las curvas elípticas definidas sobre cuerpos finitos proporcionan grupos finitos abelianos, donde los cálculos se efectúan con la eficiencia que requiere un criptosistema, y donde el cálculo de logaritmos es aún más difícil que en los cuerpos finitos. Además, existe mayor facilidad para escoger una curva elíptica que para encontrar un cuerpo finito, lo que da una ventaja más frente a su predecesor, el sistema de El Gamal.

Sistema de McEliece.

Se basa en la teoría de la codificación algebraica, utilizando el hecho de que la decodificación de un código lineal general es un problema NP-completo.

Sistema RSA

La seguridad del RSA se basa en el hecho de que no existe una forma eficiente de factorizar números que sean productos de dos grandes primos.

Fue desarrollado en 1977 por Ronald Rivest, Adi Shamir y Leonard Adleman, de ahí el nombre de RSA, que corresponde a las iniciales de los apellidos de sus autores.

En la siguiente descripción del algoritmo señalamos entre paréntesis que partes del sistema se consideran publicas y cuales secretas.

Encontrar dos grandes números primos, p y q (secretos), y calcular el número n (publico) mediante su producto, n=p*q.

Encontrar la clave de descifrado constituida por un gran número entero impar, d (secreto), que es primo con el número F(n) (secreto), obtenido mediante F(n)=(p-1)*(q-1). Siendo F(n) la función de Euler.
Calcular el entero e (publico) tal que 1 ó e ó F(n), mediante la formula: e*d-1(mod F(n)).
Hacer publica la clave de cifrado (e,n).
Para cifrar un texto, es necesario previamente codificar el texto en un sistema numérico, bien decimal o bien binario, y dividir en bloques Mi de tamaño j o j-1 de forma que, según sea el alfabeto usado el decimal o el binario cumpla en cada caso: $10^{(j-1)} < n < 10^j$ o $2^{(j-1)} < n < 2^j$. Cuando se toma como tamaño j, el descifrado del texto puede no ser único, por tanto esta elección se hace solo cuando la unicidad del descifrado no es importante.
Cifrar cada bloque Mi transformándolo en un nuevo bloque de números Ci de acuerdo con la expresión: Ci-Mi^e(mod n).
Para descifrar el bloque Ci, se usa la clave privada d según la expresión: Mi-Ci^d(mod n).

Pretty Good Privacy(PGP)

Es un programa de cifrado híbrido. Combina el cifrado simétrico y asimétrico, cogiendo lo bueno de ambos. Es decir, creamos una clave simétrica y ciframos el mensaje con ella, para ganar en velocidad. Y después, ciframos la clave simétrica con la clave pública del destinatario, logrando así mandar de forma segura la clave simétrica al destinatario.
Lo que se hace es usar la clave pública para cifrar, pero no el mensaje, sino la clave simétrica con la que va encriptado el mensaje. También, se pueden cifrar diferentes mensajes con diferentes claves, lo que hará que la comunicación sea más segura que si todos nuestros mensajes se cifran con la misma clave.

Registro De Acceso Al Sistema

Hoy en día es requisito en toda organización es necesario tener un sistema de control de accesos apropiado para llevar un control estricto de los usuarios que ingresan al sistema de computo. Esto representa una medida de seguridad para evitar que individuos no autorizados tengan libre acceso, o bien, para llevar un mejor control de los usuarios que acceden al sistema registrando su nick, la hora, etc.
También es necesario llevar un control de los intentos de accesos inválidos para una mayor seguridad en caso de alguna acción en contra del sistema de información

Registros De Intentos De Acceso

Los registros serán muy útiles para los administradores del sistema para prevenir o como base de cualquier incidente de seguridad relacionado con los sistemas de información, así se les facilitara la investigación y sabrán que usuario intento acceder de forma ilícita

Estos registros podrán ser creados siempre que exista un Sistema de Control de Accesos apropiado. Todos los registros especificados en esta sección tienen que ser guardados

Tienen que establecerse controles para poder limitar el número de intentos fallidos de conexión al sistema, incluyendo el bloqueo del identificador de usuario, cuando se sobrepase el límite preestablecido por contraseña inválida.

El departamento de Sistemas de Información tiene que tener definido e implantado un proceso que le permita obtener informes de los intentos fallidos de acceso al sistema, cuando sean solicitados.

Registros de Actividades

El registro de actividades será de mucha utilidad para el control de la seguridad de la información ya que registrara todas las actividades que realizo el usuario.

El registro de actividades servirá para identificar al usuario si realizo alguna actividad ilícita en contra del sistema de información.

El registro de actividades también servirá como base para una auditoria informática y estos registros deberán guardarse como pruebas de algún acto en contra de la información.

Informes

El departamento de Sistemas de Información tiene que tener definido e implantado un proceso o controles que le permita crear informes con todas las actividades realizadas por los usuarios, él numero de accesos al sistema y el registro de accesos fallidos al sistema para llevar un mejor control de la seguridad en el centro de computo.

CONTROL DE ACCESO EXTERNO

Mantener los niveles de protección de los Sistemas de Información cuando, de forma autorizada, sean accedidos por usuarios ajenos a la empresa o por empleados en conexión desde terminales no controlados por la empresa.
Las facilidades que la informática y las comunicaciones ofrecen a los usuarios, permiten ampliar cada vez más el campo de acción y la obtención de información conectándose a redes externas públicas que ofrecen servicios de proceso, red e información.

Al mismo tiempo, las empresas van estableciendo acuerdos de colaboración que implican la autorización de acceso y utilización de Recursos Informáticos y Activos de Información, bajo determinadas condiciones y en los que la conexión telemática es imprescindible.
Por todo lo anterior, se deduce que, al utilizar una red de comunicaciones externa y no controlada por la empresa, se están utilizando facilidades que pueden representar un riesgo para los Sistemas de Información de la empresa.
A continuación se incluye la descripción de algunos conceptos que van a ser usados en este capítulo, y al final del mismo un glosario de términos que puede ser de utilidad para su mejor comprensión.

Seguridad De Red

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Estas se deben proteger con cuidado. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella, e incluso imprimirla.
Por supuesto, una red deja de ser eficiente si se convierte en una fortaleza inaccesible. El administrador de la red tal vez tenga que clasificar a los usuarios de la red con el objeto de adjudicarles el nivel de seguridad adecuado. A continuación se sugiere un sistema en tres niveles:

Nivel de administración_ellos que diseñan, mantienen o ponen en marcha la red. Este debe estar constituido sólo por el administrador o por un pequeño grupo de personal de soporte y administración.

Usuarios fiables. Aquellos usuarios que cumplen las normas y cuyo trabajo se pueda beneficiar de una mayor libertad de acceso a la red.

Usuarios vulnerables. Aquellos que muestran falta de competencia, son excesivamente curiosos o beligerantes, o los que por alguna razón no se puede confiar.

Estos niveles pueden tener un reflejo en el número de barreras que se establecen para el acceso al sistema y el tipo de derechos de acceso que se conceden, para cuando se ha obtenido la conexión, así como el nivel de supervisión y la frecuencia de las comprobaciones

Estaciones de trabajo sin flopy disk. Una posible solución para poder impedir la copia de programas y datos fuera de la red en disquetes, y que a través de los disquetes ingresen virus y otros programas dañinos a la red, es dotar a los usuarios vulnerables con estaciones de trabajo sin flopy disk.

Control De Acceso A La Red

- . Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- . Restringir las posibilidad de conectar estaciones mediante llaves, tarjetas de identificación, tarjetas inteligentes y sistemas biométricos.
- Identificación para la red con clave de acceso.
- . Protección con clave de todas la áreas sensitivas de datos y restricción de acceso a los programas, según su uso.
- Registro de toda la actividad de la estación de trabajo.
- . Protección con clave de acceso o bloqueo de todas las operaciones de copia a disquete en las estaciones de trabajo.
- Monitorización de todas las operaciones de copia en disquete en las estaciones de trabajo.

Protección Del Servidor

La parte más importante de la red es el servidor. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades.

La dependencia en que esté el servidor no debe ser accesible para nadie, excepto para el administrador de la red. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él. Las impresoras y otros periféricos deben mantenerse alejados de ojos fisgones.

Dada la importancia del servidor y la cantidad de datos que pasan por él, es necesario efectuar copias de seguridad, del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).

Firewall

Un firewall es simplemente un filtro que controla todas las comunicaciones que pasan de una red a la otra y en función de lo que sean permite o deniega su paso. Para permitir o denegar una comunicación el firewall examina el tipo de servicio al que corresponde, como pueden ser el web, el correo o el IRC. Dependiendo del servicio el firewall decide si lo permite o no. Además, el firewall examina si la comunicación es entrante o saliente y dependiendo de su dirección puede permitirla o no.

De este modo un firewall puede permitir desde una red local hacia Internet servicios de web, correo y TFP, pero no a IRC que puede ser innecesario para nuestro trabajo. También podemos configurar los accesos que se hagan desde Internet hacia la red local y podemos denegarlos todos o permitir algunos servicios como el de la web, (si es que poseemos un servidor web y queremos que accesible desde Internet). Dependiendo del firewall que tengamos también podremos permitir algunos accesos a la red local desde Internet si el usuario se ha autentificado como usuario de la red local.

Un firewall puede ser un dispositivo software o hardware, es decir, un aparatito que se conecta entre la red y el cable de la conexión a Internet, o bien un programa que se instala en la máquina que tiene el modem que conecta con Internet. Incluso podemos encontrar ordenadores computadores muy potentes y con software específico que lo único que hacen es monitorizar las comunicaciones entre redes

Un Sistema Firewall está compuesto por:

- un Sistema de Filtro de Paquetes (Packet Filter System) y
- Un Sistema de Servicios (Services System).

Sistema De Filtro De Paquetes

El sistema de filtrado de paquetes rutea paquetes entre host internos y externos, pero de manera selectiva. Permite bloquear cierto tipo de paquetes de acuerdo con la política de seguridad de la red. El tipo de ruteo usado para filtra paquetes en un Firewall es conocido como "screening router".

Se puede selectivamente rutear paquetes desde o hacia su sitio:

1. Bloquear todas las conexiones que entran desde sistemas externos, excepto las conexiones SMTP (solo recibirá mail)
2. Bloquear todas las conexiones que provienen de un determinado lugar que se considera peligroso
3. Permitir servicio de Mail y FTP, pero bloqueando servicios peligrosos como TFTP, RPC, sercios "r" (rlogin, rsh, etc), etc.

Sistema de Servicios (Services System).

Los servicios Proxy son aplicaciones o programas servidores que corren en un Host Firewall.

Proxy es un sistema intermediario entre hosts internos de una red y los host de Internet de forma tal que reciba las requisiciones de unos y se las pase a los otros previa verificación de accesos y privilegios.

Los sistemas Proxy son efectivos solo si se utilizan junto a métodos de restricción de tráfico IP entre clientes y servidores reales. De este modo, un cliente no podrá "bypasear" el servidor Proxy para comunicarse con un servidor real utilizando este protocolo.

El programa cliente del usuario se comunica con el servidor Proxy enviando pedido de conexión con un servidor real. El servidor Proxy evalúa esta requisición y decide si se permitirá la conexión.

Si el servidor Proxy permite la conexión, envía al servidor real la solicitud recibida desde el cliente. De este modo, un servidor Proxy se ve como "Servidor" cuando acepta pedidos de clientes y como "cliente" cuando envía solicitudes a un servidor real.

Una vez que establecida la comunicación entre un cliente y un servidor real, el servidor Proxy actúa como un retransmisor pasando comandos y respuestas de un lado a otro.

La comunicación entre el programa cliente y el servidor Proxy puede realizarse de dos formas distintas:

Custom Client Software: El cliente debe saber como opera el servidor Proxy, como contactarlo, como pasar la información al servidor real,.

Custom User Procedures: El usuario utiliza un cliente standard para conectarse con un servidor Proxy y usa diferentes procedimientos (comandos del servidor Proxy) para pasar información acerca del servidor real al cual quiere conectarse. El servidor Proxy realiza la conexión con el servidor real

Tipos de Firewall

Filtros A Nivel Paquete (Packet Filters):

Esta tecnología pertenece a la primera generación de firewalls la cual analiza el tráfico de la red. Cada *paquete* que entra o sale de la red es inspeccionado y lo acepta o rechaza

basándose en las reglas definidas por el usuario. El filtrado de paquetes es efectivo y transparente para los usuarios de la red, pero es difícil de configurar. Además de que es susceptible a *IP Spoofing*.

Las reglas para rechazar o aceptar un *paquete* son las siguientes:
• Si no se encuentra una regla que aplicar al *paquete*, el *paquete* es rechazado.
• Si se encuentra una regla que aplicar al *paquete*, y la regla permite el paso, se establece la comunicación.
• Si se encuentra una regla que aplicar al *paquete*, y la regla rechaza el paso, el *paquete* es rechazado.

Firewall A Nivel Circuito (Circuit Level Firewalls):

Esta tecnología pertenece a la segunda generación de firewalls y valida que los paquetes pertenezcan ya sea a una solicitud de conexión o bien a una conexión entre dos computadoras. Aplica mecanismos de seguridad cuando una conexión *TCP* o *UDP* es establecida. Una vez que la conexión se establece, los paquetes pueden ir y venir entre las computadoras sin tener que ser revisados cada vez.
El firewall mantiene una tabla de conexiones válidas y permite que los paquetes de la red pasen a través de ella si corresponden a algún registro de la tabla. Una vez terminada la conexión, la tabla se borra y la transmisión de información entre las dos computadoras se cierra.

Firewall A Nivel Aplicación (Application Layer Firewalls):

Pertenece a la tercera generación de firewalls. Examina la información de todos los paquetes de la red y mantiene el estado de la conexión y la secuencia de la información. En este tipo de tecnología también se puede validar claves de acceso y algunos tipos de solicitudes de servicios.
La mayoría de estos tipos de firewalls requieren software especializado y servicios Proxy. Un Servicio Proxy es un programa que aplica mecanismos de seguridad a ciertas aplicaciones, tales como *FTP* o HTTP. Un servicio proxy puede incrementar el control al acceso, realizar chequeos detallados a los datos y generar auditorias sobre la información que se transmite.

Filtros Dinámicos A Nivel Paquete (Dynamic Packet Filters):

Pertenece a la cuarta generación de firewall y permite modificaciones a las reglas de seguridad sobre la marcha. En la práctica, se utilizan dos o más técnicas para configurar el firewall. Un firewall es considerado la primera línea de defensa para proteger la información privada.

Antivirus

Es un programa creado para prevenir o evitar la activación de los virus, así como su propagación y contagio. Cuenta además con rutinas de detención, eliminación y reconstrucción de los archivos y las áreas infectadas del sistema.

Un antivirus tiene tres principales funciones y componentes:

Vacuna

Es un programa que instalado residente en la memoria, actúa como "filtro" de los programas que son ejecutados, abiertos para ser leídos o copiados, en **tiempo real**.

Detector

Es el programa que examina todos los archivos existentes en el disco o a los que se les indique en una determinada ruta o PATH. Tiene instrucciones de **control** y **reconocimiento** exacto de los códigos virales que permiten capturar sus pares, debidamente registrados y en forma sumamente rápida desarman su estructura.

Eliminador

Es el programa que una vez desactivada la estructura del virus procede a eliminarlo e inmediatamente después a reparar o reconstruir los archivos y áreas afectadas.

Tan grave es el problema con los virus informaticos que diversas empresas se han preocupado del tema de los virus informáticos y han creado la **A. V. P. D.** (Antivirus Product Developers, Desarrolladores de Productos Antivirus) que es una asociación formada por las principales empresas informáticas del sector, entre las que se cuentan:

- Cheyenne Software
- McAfee Associates
- I. B. M.
- Intel
- Symantec Corporation.
- ON Tecnology
- Stiller Research Inc.
- S&S International
- ThunderByte

Bloqueo De Puertos

Son programas que escanean y te permiten cerrar el paso a los puertos (que tengas abiertos) Y que quieras tener cerrados

Los puertos son los puntos de enganche para cada conexión de red que realizamos. El protocolo TCP (el utilizado en Internet) identifica los extremos de una conexión por las direcciones IP de los dos nodos (ordenadores) implicados (servidor y cliente) y el número de los puertos de cada nodo.

Una políticas de seguridad de cualquier máquina conectada a Internet o a una red comienzan por un escaneado de puertos, con objeto de determinar sus puertas de entrada. Únicamente deben estar abiertos los puertos que sean imprescindibles para el funcionamiento.
Otra medida de seguridad para no ser un blanco fácil para ataques de denegación de servicios (Dos). Estos puertos deben ser cerrados en prácticamente todas las situaciones. Entre ellos se encuentran: echo (7), discard (9), systat (11), daytime (13), netstat (15), chargen (19), bootp (67), tftp (69), finger (79), pop-2 (109) y uucp (117). Y, en general, deben ser cerrados aquellos puertos que no sean imprescindibles como por ejemplo el puerto http (80), si nuestra máquina no es un servidor web. De esta forma evitaremos que un *hacker* se introduzca en nuestro ordenador utilizando algún agujero de seguridad conocido (asociado a algún servicio o puerto concreto) y obtenga informaciones valiosas.

Existen paginas en Internet que ofrecen un servicio de escaneo de puertos para determinar tanto la presencia de programas maliciosos (troyanos), como la de potenciales agujeros de seguridad (puertos abiertos de servicios que no se utilizan). El cual te puede ser muy útil para saber que tan segura es tu conexión a Internet y así tomar medidas de seguridad.). El escáner también indica si los puertos están protegidos por cortafuegos (*firewalled* o *stealthed*), o no.
www.grc.com , www.hackerwhacker.com www.seguridad.internautas.org/3C/es/scan-online www.worldseth.com

Monitoreo De La Red

Son programas de monitoreo de la red que le permitirá al administrador verificar el estado general o particular de la red y de igual manera el estado de los equipos; en caso de presentarse problemas en alguno se avisará al administrador responsable del equipo.
También se facilita la instalación y configuración de equipos de cómputo personal proporcionando un mejor tiempo de respuesta y disponibilidad de los equipos. Sus funciones primarias son:

- El monitoreo de un sistema de red.
- Proporcionar, una descripción (opinión) simple del estado actual de la red.
- Genera alarmas sobre cambios de estado.

- Genera un reporte de cambios de estado.
- Informes generales de la red.

Ejemplos de programas para el monitoreo de redes:

- Hp-Network Node Manager
- Host Monitor
- Analogx Netstat Live

Conexiones Seguras(ssl)

Toda transacción segura por la red debe contemplar los aspectos de Autenticidad, Integridad, Confidencialidad y No Repudio. Son varios los sistemas y tecnologías que se han desarrollado para intentar implementar estos aspectos en las transacciones electrónicas, siendo sin duda SSL el más conocido y usado en la actualidad. SSL permite la Confidencialidad y la Autentificación en las transacciones por Internet, siendo usado principalmente en aquellas transacciones en la que se intercambian datos sensibles, como números de tarjetas de crédito o contraseñas de acceso a sistemas privados. SSL es una de las formas base para la implementación de soluciones PKI (Infraestructuras de Clave Pública).

Secure Socket Layer es un sistema de protocolos de carácter general diseñado en 1994 por la empresa Nestcape Communcations Corporation, y está basado en la aplicación conjunta de Criptografía Simétrica, Criptografía Asimétrica (de llave pública), certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet. De los sistemas criptográficos simétricos, motor principal de la encriptación de datos transferidos en la comunicación, se aprovecha la rapidez de operación, mientras que los sistemas asimétricos se usan para el intercambio seguro de las claves simétricas, consiguiendo con ello resolver el problema de la Confidencialidad en la transmisión de datos.

SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socked (nombre de máquina más puerto), de forma transparente al usuario y a las aplicaciones que lo usan.

Actualmente es el estándar de comunicación segura en los navegadores web más importantes (protocolo HTTP), como Nestcape Navigator e Internet Explorer, y se espera que pronto se saquen versiones para otras otros protocolos de la capa de Aplicación (correo, FTP, etc.).

La identidad del servidor web seguro (y a veces también del usuario cliente) se consigue mediante el Certificado Digital correspondiente, del que se comprueba su validez antes de

iniciar el intercambio de datos sensibles (Autenticación), mientras que de la seguridad de Integridad de los datos intercambiados se encarga la Firma Digital mediante funciones hash y la comprobación de resúmenes de todos los datos enviados y recibidos.

Software De Análisis

Son herramientas de análisis que sirven para detectar fallas en la seguridad de nuestra red o conexión a Internet, también para detectar posibles virus e intentos de ataques por parte de hackers y para optimizar el rendimiento de nuestros equipos de computo.

Niveles De Seguridad

Las medidas de seguridad de la información son el conjunto de medidas de carácter técnico y organizativo que debe implantar el Responsable de la información, a fin de garantizar la seguridad de los centros de computo, en los que se ubican físicamente los ficheros de datos, de los equipos, sistemas informáticos y programas que se utilicen en su almacenamiento y tratamiento, y de las personas que realizan las labores de recogida y tratamiento de los datos.

En la Seguridad se establecen **tres niveles de seguridad** o niveles de protección de la información según la naturaleza de los datos.

Nivel Básico: Es el conjunto de medidas de seguridad que deben adoptar la información automatizada de los datos de carácter personal, cualquiera que sea el tipo o la naturaleza de los datos incluidos en el fichero.

Nivel Medio: Es el conjunto de medidas de seguridad que deben adoptar los archivos automatizados que contengan datos de carácter personal que se refieran a alguna de las siguientes materias:

- Datos sobre comisión de infracciones administrativas o penales.
- Datos relativos a la Hacienda Pública.
- Datos sobre servicios financieros.
- Datos de carácter personal que considerados en conjunto sean suficientes para obtener una evaluación de la personalidad del interesado

Nivel Alto: Es el conjunto de medidas de seguridad que deben adoptar los archivos automatizados que contengan los siguientes tipos de datos:

- Datos relativos a la ideología, religión, creencias, origen racial, salud o vida sexual.
- Datos recabados con fines policiales sin el consentimiento de los interesados

Ataques Remotos

Escaneo De Puertos

Una de las primeras actividades que un potencial (o no tan potencial) atacante realizará contra su objetivo será sin duda un escaneo de puertos, un *portscan*; esto le permitirá obtener en primer lugar información básica acerca de qué servicios estamos ofreciendo en nuestras máquinas y, adicionalmente, otros detalles de nuestro entorno como qué sistema operativo tenemos instalados en cada *host* o ciertas características de la arquitectura de nuestra red. Analizando qué puertos están abiertos en un sistema, el atacante puede buscar agujeros en cada uno de los servicios ofrecidos: cada puerto abierto en una máquina es una potencial puerta de entrada a la misma.

Comprobar el estado de un determinado puerto es *a priori* una tarea muy sencilla; incluso es posible llevarla a cabo desde la línea de órdenes, usando una herramienta tan genérica como telnet. Por ejemplo, imaginemos que queremos conocer el estado del puerto 5000 en la máquina cuya dirección IP es 192.168.0.10; si el telnet a dicho puerto ofrece una respuesta, entonces está abierto y escuchando peticiones

Podemos dividir los escaneos en tres grandes familias: *open*, *half-open* y *stealth*; vamos a hablar con más detalle de cada una de ellas y de los diferentes tipos escaneos que las forman.

Los escaneos **open** se basan en el establecimiento de una conexión TCP completa mediante el conocido como protocolo de acuerdo de tres vías o *three-way handshake* , por lo que son muy sencillos de detectar y detener. Utilizan la llamada connect(), siendo lo más similar guardado las distancias, al ejemplo del telnet que hemos visto antes: el escaneador intenta establecer una conexión con un puerto concreto del *host* atacado, y en función de la respuesta obtenida conoce su estado: una técnica rápida, sencilla, fiable y que no necesita de ningún privilegio especial en la máquina atacante.

La segunda técnica que hemos comentado es la de los escaneos **half-open**; en este caso, el pirata finaliza la conexión antes de que se complete el protocolo de acuerdo de tres vías, lo que de entrada dificulta - - aunque no mucho - la detección del ataque por parte de algunos detectores de intrusos muy simples (casi todos los actuales son capaces de detectarlos). Dentro de esta técnica se encuentra el *SYN Scanning*: cuando el origen - atacante - recibe

del destino - máquina escaneada - los *bits* SYN+ACK, envía un *bit* RST (no es necesaria una nueva trama, ya que este *bit* se envía automáticamente a nivel de núcleo) en lugar del ACK correspondiente a un *three-way handshake* completo. Los escaneos SYN son fácilmente detectables y pueden ser bloqueados en cualquier cortafuegos; Existe una variable de esta técnica denominada *dumb scanning* en la que entra en juego una tercera máquina denominada `tonta' (por el poco tráfico que emite y recibe), algo que puede ayudar al pirata a camuflar su origen real. Sin embargo, el *dumb scanning* es más complicado que el *SYN scanning*, por lo que se utiliza mucho menos en la vida real.

Finalmente, existe otra modelo de escaneo denominado **stealth scanning**. En diciembre de 1995 Christopher Klaus proporcionó las pautas de ciertas técnicas de escaneo que permitían al atacante eludir la acción de los sistemas de detección de intrusos de la época y a las que bautizó como *stealth scanning*; actualmente el significado del término ha cambiado, ya que lo que Klaus presentó se denomina hoy en día *half-open scanning*, y por *stealth scanning* se conoce a una familia de técnicas de escaneo que cumplen alguna de las siguientes condiciones

- Eludir cortafuegos o listas de control de acceso.
- No ser registradas por sistemas de detección de intrusos, ni orientados a red ni en el propio *host* escaneado.
- Simular tráfico normal y real para no levantar sospechas ante un analizador de red.

Spoofing

Por *spoofing* se conoce a la creación de tramas TCP/IP utilizando una dirección IP falsa; la idea de este ataque - al menos la idea - es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del *host* suplantado. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún demasiado abundantes (no tenemos más que pensar en los comandos r-, los accesos NFS, o la protección de servicios de red mediante *TCP Wrapper*), el *spoofing* sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización.

Para evitar ataques de *spoofing* exitosos contra nuestros sistemas podemos tomar diferentes medidas preventivas; en primer lugar, parece evidente que una gran ayuda es reforzar la secuencia de predicción de números de secuencia TCP
Otra medida sencilla es eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas; el cifrado y el filtrado de las conexiones que pueden aceptar nuestras máquinas también son unas medidas de seguridad importantes de cara a evitar el *spoofing*.

existen otros ataques de falseamiento relacionados en mayor o menor medida con este, entre los que destacan el *DNS Spoofing*, el *ARP Spoofing* y el *Web Spoofing*

- *DNSSpoofing*
  Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP). Esto se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como *DNS Poisoning*); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.
- *ARPSpoofing*
  El ataque denominado *ARP Spoofing* hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un *host* atacante en lugar de hacerlo a su destino legítimo. La idea es sencilla, y los efectos del ataque pueden ser muy negativos: desde negaciones de servicio hasta interceptación de datos, incluyendo algunos *Man in the Middle* contra ciertos protocolos cifrados.
- *WebSpoofing*
  Este ataque permite a un pirata visualizar y modificar cualquier página *web* que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL. Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado - incluyendo las cargadas en nuevas ventanas del navegador - a través de su propia máquina, donde son modificadas para que cualquier evento generado por el cliente sea registrado (esto implica registrar cualquier dato introducido en un formulario, cualquier *click* en un enlace, etc.).

Negaciones De Servicio

Las negaciones de servicio (conocidas como Dos, *Denial of Service*) son ataques dirigidos contra un recurso informático (generalmente una máquina o una red, pero también podría tratarse de una simple impresora o una terminal) con el objetivo de degradar total o parcialmente los servicios prestados por ese recurso a sus usuarios legítimos; constituyen en muchos casos uno de los ataques más sencillos y contundentes contra todo tipo de servicios, y en entornos donde la disponibilidad es valorada por encima de otros parámetros de la seguridad global puede convertirse en un serio problema, ya que un pirata puede interrumpir constantemente un servicio sin necesidad de grandes conocimientos o recursos, utilizando simplemente sencillos programas y un módem y una computadora.

los ataques de negación de servicio distribuidos más habituales consisten en el envío de un gran número de paquetes a un determinado objetivo por parte de múltiples *hosts*, lo que se conoce como *packet flooding*

Ataques A Aplicaciones

Correo Electrónico

El enorme crecimiento en la adopción del correo electrónico a lo largo de los años ha venido acompañado por el desarrollo de código malicioso, es decir, virus y ataques de correo. El SMTP se ha convertido para hackers y crackers en una forma sencilla de distribuir el contenido peligroso en la red local. Las redes corporativas han sido sembradas de gusanos y virus, así como de crackers, a través del protocolo de correo. Un cortafuegos típico no puede protegernos contra tales ataques de correo electrónico, simplemente porque no analiza el correo, ni su contenido.
Como los mensajes de correo pueden incluir archivos adjuntos, los hackers pueden enviar archivos infectados y esperar que el destinatario lo abrirá, como ocurrió con Melissa y Manwella. Este método utiliza ingeniería social para impulsar al usuario final a ejecutar el archivo. Además hay otros métodos que permiten a un experto, y posiblemente maligno cracker, incluir código en el correo y ejecutar automáticamente aplicaciones a medida, mientras el usuario final lee el texto del correo. Tales problemas ocurren desde que se utiliza el HTML en los correos y ha sido aprovechado por célebres gusanos como KaK worm, BubbleBoy virus o el más reciente Nimda.
A pesar de que los productos anti-virus pueden atrapar muchos virus y gusanos, los hackers están capacitados para evitar tales protecciones produciendo su propio código a la medida. Como resultado pueden penetrar la red corporativa peligrosas amenazas a través de unos métodos poco conocidos y saltándose la protección anti-virus y otras protecciones anti-hacker tradicionales. La posible amenaza de los hackers a la red interna es tan grande como baja es la seguridad de la red interna para asegurar su uso.

Ataques Vía Web

Los ataques a las páginas *web* de una organización son casi siempre los más `vistosos' que la misma puede sufrir: en cuestión de minutos los hackers de todo el mundo se enteran de cualquier problema en la página *web* principal de una empresa más o menos grande pueda estar sufriendo, y si se trata de una modificación de la misma incluso existen recopilatorios de páginas *`hackeadas'*. Por supuesto, la noticia de la modificación salta inmediatamente a los medios, que gracias a ella pueden rellenar alguna cabecera sensacionalista sobre `los piratas de la red', y así se consigue que la imagen de la empresa atacada caiga notablemente y la del grupo de piratas suba entre la comunidad *'underground'* nacional o internacional.

La mayor parte de estos ataques tiene éxito gracias a una configuración incorrecta del servidor o a errores de diseño del mismo: si se trata de grandes empresas, los servidores

web suelen ser bastante complejos (alta disponibilidad, balanceo de carga, sistemas propietarios de actualización de contenidos...) y difíciles de administrar correctamente, mientras que si la empresa es pequeña es muy posible que haya elegido un servidor *web* simple en su instalación y administración pero en el cual es casi imposible garantizar una mínima seguridad: sí, hablamos de *Microsoft Internet Information Server*, un sistema que reconocidos expertos en seguridad han recomendado públicamente **no utilizar** en entornos serios. Sea por el motivo que sea, la cuestión es que cada día es más sencillo para un hacker ejecutar órdenes de forma remota en una máquina, o al menos modificar contenidos de forma no autorizada, gracias a los servidores *web* que un sistema pueda albergar.

Ataques potenciales

Ingeniería Social

Bajo el nombre de Ingeniería Social (literalmente traducido del inglés Social Engineering) se encuentran comprendidas todas aquellas conductas útiles para conseguir información de las personas cercanas a una computadora. Es una disciplina que consiste, ni más ni menos en sacar información a otra persona sin que esta sé de cuenta de que te esta revelando "información sensible".

Hoy en día sólo son necesarias las malas intenciones y una conexión a Internet para sembrar el caos. Ya no es cuestión de conocimientos, sobre todo teniendo en cuenta que en los sistemas operativos más populares, se antepone la comodidad a la seguridad del sistema mismo. La mayoría de los ataques a la seguridad se deben a errores humanos y no a fallas electrónicas. Los intrusos usan "ingeniería social" para acceder a los sitios, y siempre alguien los deja entrar sin ningún problema.

Tradicionalmente, los intrusos se han valido de los engaños para conseguir atacar al eslabón más débil de la cadena de usuarios y responsables de un equipo de cómputo o de una red. De nada vale encriptar las comunicaciones, sellar los accesos, diseñar un buen esquema de seguridad para las distintas estaciones de trabajo y jerarquizar convenientemente los accesos a los mismos si no contamos con un personal que se halle lo suficientemente preparado para hacerle frente los engaños externos.

La principal herramienta que manejan actualmente los creadores de virus es la que se ha dado en llamar ingeniería social. Con este curioso término se engloba una serie de tretas, artimañas y engaños elaborados cuyo fin es confundir al usuario o, peor todavía, lograr que comprometa seriamente la seguridad de sus sistemas. Esto no es un conocimiento exacto pero, al ponerse en práctica con un grupo tan elevado de posibles víctimas, el éxito casi siempre está garantizado. Aprovechando sentimientos tan variados como la curiosidad, la

avaricia, el sexo, la compasión o el miedo, el vándalo interesado consigue su objetivo, una acción por parte del usuario.

Un claro ejemplo de Ingeniería Social más común es el de alguien que llama por teléfono a una empresa para decir que necesita ayuda o hablar con el administrador de la red porque hay que modificar algún aspecto de la configuración. Durante la conversación, y a través de escogidas y cuidadas preguntas, el atacante obtendrá los datos (como los códigos de acceso a los equipos) que necesita para vulnerar la seguridad de todo el corporativo.

La ingeniería social es una acción muy simple, pero peligrosa. Los "hackers" llaman a los centros de datos y fingen ser un cliente que perdió su contraseña, o se dirigen a un sitio y esperan que alguien deje la puerta abierta. Otras formas de ingeniería social no son tan obvias. Los "hackers" son conocidos por crear sitios Web, concursos o cuestionarios falsos que piden a los usuarios que ingresen una contraseña. Si un usuario escribe la misma contraseña que usa en su trabajo, el hacker puede ingresar en las instalaciones sin tener que descifrar ni siquiera una línea de código.

Con el objetivo de infectar el mayor número posible de equipos, cada vez son más los gusanos que recurren a la Ingeniería Social, habitualmente empleada por los creadores de código malicioso para engañar a los usuarios. En la Ingeniería Social no se emplea ningún programa de software o elemento de hardware, sólo grandes dosis de ingenio, sutileza y persuasión para así lograr obtener información a través de otra persona sin que se dé cuenta de que está revelando información importante con la que, además, el atacante puede dañar su computadora.

En la práctica, los autores de virus (gusanos o troyanos) emplean la Ingeniería Social para que sus creaciones se propaguen rápidamente. Para ello atraen la atención del usuario y consiguen que realice alguna acción que, normalmente, consiste en inducirlo a que abra algún archivo que es el que procede a realizar la infección. De hecho, la mayoría de las pérdidas provocadas por los efectos de los códigos maliciosos tienen su origen en la ignorancia u omisión de políticas de seguridad.

El personal de una empresa debería de seguir las siguientes recomendaciones para evitar caer víctima de las trampas de la Ingeniería Social:

1. - Antes de abrir los correos analizarlos con un antivirus eficaz y debidamente actualizado, ya que cualquier mensaje de correo electrónico puede contener códigos maliciosos aunque no le acompañe el símbolo de datos adjuntos.

2. - Nunca ejecutar un programa de procedencia desconocida, aun cuando previamente sea verificado que no contiene virus. Dicho programa puede contener un troyano o un sniffer que reenvíe nuestra clave de acceso.

3. - Los usuarios no necesitan tener acceso a todo tipo de ficheros ya que no todos son necesarios para su trabajo habitual, por ello puede ser conveniente por parte del administrador bloquear la entrada de ficheros con extensiones ".exe",".vbs", etc.

4. - Nunca informe telefónicamente de las características técnicas de la red, sus localizaciones espaciales o personas a cargo de la misma. En su lugar lo propio es remitirlos directamente al responsable del sistema.

5.- Controlar los accesos físicos al lugar donde se hallan los servidores o terminales desde los que se puede conectar con los servicios centralizados de control.

6.- Nunca tirar documentación técnica a la basura, sino destruirla.

7.- Verificar previamente la veracidad de la fuente que solicite cualquier información sobre la red, su localización en tiempo y espacio y las personas que se encuentran al frente de la misma.

8.- En caso de existir, instalar los parches de actualización de software que publican las compañías para solucionar vulnerabilidades. De esta manera se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.

10.- Controlar que las anteriores instrucciones se cumplen sistemáticamente.

Shoulder

Otro tipo de ataque relacionado con la ingenuidad de los usuarios del sistema (pero también con el control de acceso físico) es el denominado *shoulder surfing*. Consiste en `espiar' físicamente a los usuarios, para obtener generalmente claves de acceso al sistema. Por ejemplo, una medida que lamentablemente utilizan muchos usuarios para recordar sus contraseñas es apuntarlas en un papel pegado al monitor de su PC o escribirlas en la parte de abajo del teclado; cualquiera que pase por delante del puesto de trabajo, sin problemas puede leer el *login*, *password* e incluso el nombre de máquina a la que pertenecen. Esto, que nos puede parecer una gran tontería, por desgracia no lo es, y se utiliza más de lo que muchos administradores o responsables de seguridad piensan; y no sólo en entornos `privados' o con un control de acceso restringido, como pueda ser una sala de operaciones de un centro de computo, sino en lugares a los que cualquiera puede llegar sin ninguna acreditación.

El *shoulder surfing* no siempre se ve beneficiado por la ingenuidad de los simples usuarios de un equipo; en determinadas ocasiones son los propios programadores (gente que teóricamente ha de saber algo más sobre seguridad que el personal de administración o de

atención al público) los que diseñan aplicaciones muy susceptibles de sufrir ataques de este tipo. Por ejemplo, en ciertas aplicaciones - especialmente algunas que se ejecutan sobre MS Windows, y que son más o menos antiguas - muestran claramente en pantalla las contraseñas al ser tecleadas. Cualquiera situado cerca de una persona que las está utilizando puede leer claramente esa clave; un perfecto ejemplo de lo que NO se debe hacer nunca.

Basurero

Esta técnica del basureo (en inglés, *scavenging*) está relacionada tanto con los usuarios como con la seguridad física de los sistemas, consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo. Él basureo puede ser físico, como buscar en cubos de basura (*trashing*, traducido también por *basureo*) listados de impresión o copias de documentos, o lógico, como analizar *buffers* de impresoras, memoria liberada por procesos, o bloques de un disco que el sistema acaba de marcar como libres, en busca de información.

Aunque esta técnica no es muy utilizada en la mayoría de entornos, hemos de pensar que si un usuario tira a la basura documentos que proporcionen información sobre nuestro sistema, cualquier potencial atacante puede aprovechar esa información para conseguir acceder al equipo; algo tan simple como una factura en la que se especifiquen números de teléfono o nombres (reales o de entrada al sistema) de usuarios puede convertirse en una valiosa información para un atacante. Además, en ocasiones ni siquiera es necesario andar revolviendo por los cubos de basura en busca de información comprometedora: la carencia de nociones básicas sobre seguridad informática hace posible que los usuarios dejen al alcance de cualquiera información vital de cara a mantener un sistema seguro. Personalmente, en un aula de informática

Él basureo no es un ataque habitual en organizaciones `normales', simplemente porque los datos con los que están trabajan no suelen ser de alta confidencialidad. De cualquier forma, si deseamos evitar problemas lo más inmediato es utilizar una máquina trituradora de papel (su precio no suele ser prohibitivo, y la inversión quizás valga la pena) para destruir toda la documentación antes de arrojarla a la basura; incluso nos puede interesar contratar los servicios de compañías dedicadas exclusivamente a la destrucción de estos soportes. En el caso de sistemas de almacenamiento lógico (discos, CD-ROM, cintas...) también es importante una correcta inutilización de los mismos para que un potencial atacante no pueda extraer información comprometedora; No suele ser suficiente el simple borrado del medio o un leve daño físico (por ejemplo, partir un CD-ROM), ya que como comentaremos al hablar de recuperación de datos existen empresas capaces de extraer hasta el último *BIT* de un medio borrado o dañado. Lo más efectivo sería un borrado seguro, seguido de una destrucción física importante que haga imposible la reconstrucción del medio.

Troyanos

Los caballos de Troya son impostores, es decir, archivos que pretenden ser benignos pero que, de hecho, son perjudiciales. Una diferencia muy importante con respecto a los virus reales es que *no* se replican a sí mismos. Los caballos de Troya contienen código dañino que, cuando se activa, provoca pérdidas, el control total de una maquina o incluso robo de datos. Para que un caballo de Troya se extienda es necesario dejarlo entrar en el sistema, entran a través de los 65535 puertos TCP/IP, por ejemplo abriendo un archivo adjunto de correo. Un ejemplo de caballo de Troya es PWSteal.Trojan.

L a diferencia de los virus y los caballos de Troya o troyanos están diseñados para obtener información privilegiada del ordenador donde son ejecutados. Así pues existen troyanos que únicamente consiguen contraseñas, otros que graban secuencias metidas en el teclado, otros que abren puertas traseras al ordenador, etc.

Los troyanos están formados por 3 partes:

Troyanos/Backdoor de acceso remoto

Tienen dos componentes principales: el programa Servidor, que se instala en el sistema de la victima y el programa Cliente que actúa en la computadora del atacante. Ambos programas establecen una relación Cliente/Servidor entre la PC infectada y la del atacante. Por medio de estos troyanos el atacante puede ejecutar remotamente en los sistemas infectados las mismas acciones que el administrador de un Servidor o usuarios de las PC involucradas.

Troyano/Backdoor Cliente

El Cliente se encuentra en el equipo del atacante y generalmente tiene una interfaz con opciones y desde las cuales puede ejecutar las funciones que se hayan programado para que interactúen con los sistemas de las víctimas.

Troyano/Backdoor Servidor

El Servidor que se instala en el sistema de la victima, es un programa que ocupa muy poco espacio y está asociado al Cliente, para poder recibir las instrucciones o través del mismo, ejecutar las funciones que el intruso esté facultado.

Los troyanos/backdoor se pueden transmitir por diversos medios:

Mensajes de Correo

Son la forma más fácil de propagación por medio de un archivo anexado al mensaje y si el receptor comete el error de ejecutarlo, instalará el Servidor, permitiendo que el intruso pueda controlar el o los equipos infectados.

Telnet

Funcionan en modo Cliente/Servidor y permite ejecutar comandos en el equipo infectado.

Otros servicios de Internet (HTTP, FTP, ICQ, Chat, Mensajería Instantánea)

Es posible visitar una página web en Internet, la misma que descargue automáticamente un troyano Backdoor Servidor y el sistema quedará infectado, bajo control del troyano Cliente. Del mismo modo podrá ocurrir en servidores **FTP**. Por lo general estos servidores, al ser reportados, serán deshabilitados por su ISP, en caso contrario el Proveedor de Servicios de Internet será merecedor a una sanción.

La popularidad del uso del **Chat** o de los servicios de Mensajería Instantánea, como **MSN Messenger**, **Yahoo Messenger**, **Netscape** o **AOL Messenger**, entre otros, han hecho posible la transmisión de virus, macro virus, gusanos, troyanos y backdoors, entre los usuarios conectados en una misma sesión.

Los más conocidos últimamente son el BackOrifice, Maverick's Matrix, Bunker-Hill Trojan, Subseven y el NetBus. Ambos son troyanos que abren una puerta trasera a un equipo basado en Windows 95, Windows 98 o Windows NT.

Virus

Es un programa que se puede introducir en nuestro ordenador de formas muy diversas. Este tipo de programas, los virus, son especiales ya que pueden producir efectos no deseados y nocivos. Una vez el virus se haya introducido en el ordenador, se colocará en lugares desde los que el usuario pueda ejecutarlos de manera no intencionada. Hasta que no se ejecuta el programa infectado o se cumple una determinada condición -condición de activación (una fecha concreta, una acción que realiza el usuario,...)-, el virus no actúa. Incluso en algunas ocasiones, los efectos producidos por éste, se aprecian tiempo después de su ejecución (payload). Una característica típica de los virus es su capacidad de replicarse y propagarse a otros ficheros o programas.

El nombre de virus informático es debido a su parecido con los virus biológicos. De la misma forma que los virus biológicos, los virus informáticos se introducen en el cuerpo humano (en el ordenador) de alguna forma concreta e infectan las células (archivos),

presentando algún síntoma de esta infección. Además, ambos pueden reproducirse y propagarse, extendiendo la infección desde el sistema ya infectado a otros.

Los efectos que produce un virus pueden ser destructivos o simplemente molestos: dañar o borrar los datos almacenados en un ordenador, provocar el bloqueo del equipo afectado, mostrar mensajes en pantalla,... etc.

Además de contar con técnicas de propagación e infección, en la actualidad existen virus que también utilizan técnicas de "evasión". Esto quiere decir que el virus cuenta con técnicas o sistemas de defensa que le permiten dificultar su detección y evitar las acciones que se llevan a cabo contra él.

Es importante destacar que el potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.

La definición más simple y completa que hay de los virus corresponde al modelo D. A. S., y se fundamenta en tres características, que se refuerzan y dependen mutuamente. Según ella, un virus es un programa que cumple las siguientes pautas:

- Es dañino
- Es autoreproductor
- Es subrepticio

Asimismo, se pueden distinguir tres módulos principales de un virus informático:

- Módulo de Reproducción
- Módulo de Ataque
- Módulo de Defensa

El **módulo de reproducción** se encarga de manejar las rutinas de "parasitación" de entidades ejecutables (o archivos de datos, en el caso de los virus macro) a fin de que el virus pueda ejecutarse subrepticiamente. Pudiendo, de esta manera, tomar control del sistema e infectar otras entidades permitiendo se traslade de una computadora a otra a través de algunos de estos archivos.

El **módulo de ataque** es optativo. En caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus. Por ejemplo, el conocido virus **Michelangelo**, además de producir los daños que se detallarán más adelante, tiene un módulo de ataque que se activa cuando el reloj de la computadora indica 6 de Marzo. En estas condiciones la rutina actúa sobre la información del disco rígido volviéndola inutilizable.

El **módulo de defensa** tiene, obviamente, la misión de proteger al virus y, como el de ataque, puede estar o no presente en la estructura. Sus rutinas apuntan a evitar todo aquello que provoque la remoción del virus y retardar, en todo lo posible, su detección.

Los virus se clasifican por el modo en que actúan infectando la computadora:

- Programa: Infectan archivos ejecutables tales como .com / .exe / .ovl / .drv / .sys / .bin
- Boot: Infectan los sectores Boot Record, Master Boot, FAT y la Tabla de Partición.
- Múltiples: Infectan programas y sectores de "booteo".
- Bios: Atacan al Bios para desde allí reescribir los discos duros.
- Hoax: Se distribuyen por e-mail y la única forma de eliminarlos es el uso del sentido común.

En este vinculo esta una lista de los virus del 2003

http://www.symantec.com/region/mx/avcenter/vinfodb.html

Gusanos

Los *gusanos* son programas que se replican a sí mismos de sistema a sistema sin utilizar un archivo para hacerlo. En esto se diferencian de los virus, que necesitan extenderse mediante un archivo infectado. Aunque los gusanos generalmente se encuentran dentro de otros archivos, a menudo documentos de Word o Excel, existe una diferencia en la forma en que los gusanos y los virus utilizan el archivo que los alberga. Normalmente el gusano generará un documento que ya contendrá la macro del gusano dentro. Todo el documento viajará de un equipo a otro, de forma que el documento completo debe considerarse como gusano. PrettyPark.Worm es un buen ejemplo de gusano.

Conejos

El nacimiento de los modernos virus informáticos podría encontrarse en lo que se denominó programas conejo. Un programa conejo es aquel cuya principal función, como si de un conejo se tratase, es la de reproducirse infinitamente, copiándose así mismo hasta que ocupa toda la memoria libre o el disco del ordenador, dejándolo bloqueado.
Estos programas surgieron en las redes informáticas, y se cree que sus verdaderos orígenes se encuentran cuando en los antiguos sistemas de grandes ordenadores, unos programas tenían un mayor nivel de acceso que otros. Fue entonces cuando alguien llegó a ese sistema y quiso que su programa tuviese un acceso mayor del que tenía. Como no podía hacerlo en la red, ideó un programa que, tras ponerse a la cola de los otros existentes, al llegarle el

turno se ejecutase y se copiase a sí mismo, obteniéndose así dos copias. Con estas copias sucedía lo mismo un poco más tarde, por lo que después fueron 4, 8, 16, 32, 64... etcétera. De esta forma, el programa tendría cada vez una mayor acceso (el doble que la vez anterior). Por primera vez se había creado un ingenio informático que podía ocasionar grandes catástrofes, colapsando las grandes redes informáticas.

Applets Hostiles

En los últimos años, con la proliferación de la *web*, Java y Javascript, una nueva forma de *malware* se ha hecho popular. Se trata de los denominados *applets* hostiles, *applets* que al ser descargados intentan monopolizar o explotar los recursos del sistema de una forma inapropiada ; Esto incluye desde ataques clásicos como negaciones de servicio o ejecución remota de programas en la máquina cliente hasta amenazas mucho más elaboradas, como difusión de virus, ruptura lógica de cortafuegos o utilización de recursos remotos para grandes cálculos científicos.

Aunque en un principio no se tomó muy en serio el problema de los *applets* hostiles, poco tiempo después la propia Sun Microsystems reconoció la problemática asociada y se puso a trabajar para minimizar los potenciales efectos de estos *applets*; principalmente se han centrado esfuerzos en controlar la cantidad de recursos consumidos por un programa y en proporcionar las clases necesarias para que los propios navegadores monitoricen los *applets* ejecutados. No obstante, aunque se solucionen los problemas de seguridad en el código, es probable que se puedan seguir utilizando *applets* como una forma de ataque a los sistemas: mientras que estos programas puedan realizar conexiones por red, no habrán desaparecido los problemas.

Bombas Lógicas

Las bombas lógicas son en cierta forma similares a los troyanos: Se trata de código insertado en programas que parecen realizar cierta acción útil. Pero mientras que un troyano se ejecuta cada vez que se ejecuta el programa que lo contiene, una bomba lógica sólo se activa bajo ciertas condiciones, como una determinada fecha, la existencia de un fichero con un nombre dado, o el alcance de cierto número de ejecuciones del programa que contiene la bomba; así, una bomba lógica puede permanecer inactiva en el sistema durante mucho tiempo sin activarse y por tanto sin que nadie note un funcionamiento anómalo hasta que el daño producido por la bomba ya está hecho.

Estás bombas lógicas no fueron introducidas sólo en las redes de ordenadores a través de módem, sino que también surgieron programadores que realizaban programas de encargo, e incluían bombas lógicas por si no eran pagados

En la actualidad, la mayor parte de los modernos virus contienen en su interior bombas lógicas que se activan cuando se cumple una o más de las siguientes condiciones:

- En una determinada fecha
- En una determinada hora
- Cuando un contador interno llega a un determinado número
- Cuando se cumplen ciertas características

Canales Ocultos

Un canal oculto es un cauce de comunicación que permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema; esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que *a priori* no estaría autorizado a acceder a dicha información. Los canales ocultos existen solamente en sistemas con seguridad multinivel, aquellos que contienen y manejan información con diferentes niveles de sensibilidad, de forma que se permite acceder simultáneamente a varios usuarios a dicha información pero con diferentes puntos de vista de la misma, en función de sus privilegios y sus necesidades de conocimiento (*needs to know*). El concepto de canal oculto fue introducido en 1973, en, y desde entonces muchos han sido los estudios realizados sobre este método de ataque, que afecta especialmente a sistemas en los que el aspecto más importante de la seguridad es la privacidad de los datos (por ejemplo, los militares).

Generalmente se suelen clasificar los canales cubiertos en función de varios aspectos

- Escenario
  Cuando se construyen escenarios de canales cubiertos generalmente se suele diferenciar entre canales cubiertos **de almacenamiento** y **de temporización**. Los primeros son canales en los que se utiliza la escritura directa o indirecta de datos por parte de un proceso y la lectura - también directa o indirecta - de esos datos por parte de otro; generalmente utilizan un recurso finito del sistema, como bloques de disco, que se comparte entre entidades con diferentes privilegios. Por contra, los canales ocultos de temporización utilizan la modulación de ciertos recursos, como el tiempo de CPU, para intercambiar la información entre procesos

- **Ruido**. Como cualquier canal de comunicación, oculto o no, los canales cubiertos pueden ser ruidosos o inmunes al ruido; idealmente, un canal inmune al ruido es aquél en que la probabilidad de que el receptor escuche exactamente lo que el emisor ha transmitido es 1: sin importar factores externos, no hay interferencias en la transmisión. Evidentemente, en la práctica es muy difícil conseguir estos canales tan perfectos, por lo que es habitual aplicar códigos de corrección de errores aunque éstos reduzcan el ancho de banda del canal.

- **Flujos de información**. De la misma forma que en las líneas convencionales de transmisión de datos se aplican técnicas (multiplexación en el tiempo, multiplexación en frecuencia...) para maximizar el ancho de banda efectivo, en los canales cubiertos se puede hacer algo parecido. A los canales en los que se transmiten varios flujos de información entre emisor y receptor se les denomina **agregados**, y dependiendo de cómo sé inicialicen, lean y *reseteen* las variables enviadas podemos hablar de agregación serie, paralela o híbrida; los canales con un único flujo de información se llaman **no agregados**.

Puertas Traseras

Las puertas traseras (backdoors) son programas que permiten acceso prácticamente ilimitado a un equipo de forma remota.

El problema, para quien quiere usar este ataque, es que debe convencerlo a usted de que instale el servidor. Por eso, si aparece un desconocido ofreciéndole algún programa maravilloso y tentador, no le crea de inmediato. Lo que están probablemente a punto de darle es un troyano, un servidor que le proporcionará a algún intruso acceso total a su computadora. Con todo el riesgo que esto implica, hay una forma simple y totalmente segura de evitarlo: no acepte archivos ni mucho menos ejecute programas que le hayan mandado sobre todo si son de procedencia dudosa.

Los programas que se clasifican como "backdoors" o "puertas traseras" son utilerías de administración remota de una red y permiten controlar las computadoras conectadas a ésta. El hecho que se les clasifique como software malévolo en algunos casos, es que cuando corren, se instalan en el sistema sin necesidad de la intervención del usuario y una vez instalados, no se pueden visualizar estas aplicaciones en la lista de tareas en la mayoría de los casos. Consecuentemente un backdoor puede supervisar casi todo proceso en las computadoras afectadas, desinstalar programas, descargar virus en la PC remota, borrar información, entre otras muchas cosas más.

Dada la complejidad de este tema, lo importante finalmente es comprender que si no se toman ciertas medidas mínimas, la información sensible que se encuentre en cualquier

equipo, con el simple hecho de que tenga acceso a la red de redes (Internet) es suficiente para que pueda estar expuesto a ataques de diversa índole.

Superzapping

Se denomina superzapping al uso no autorizado de un programa editor de ficheros para alterar, borrar, copiar, insertar o utilizar en cualquier forma no permitida los datos almacenados en los soportes de un ordenador. El nombre proviene de una utilidad llamada SUPERZAP diseñada para Mainframes y que permite acceder a cualquier parte del ordenador y modificarlo, su equivalente en un PC serian las Pctools o el Norton Disk Editor.

Este problema de seguridad deriva su nombre del programa `superzap`, una utilidad de los antiguos *mainframes* de IBM que permitía a quién lo ejecutaba pasar por alto todos los controles de seguridad para realizar cierta tarea administrativa, presumiblemente urgente; se trataba de un *`Rompa el cristal en caso de emergencia'* que estos sistemas poseían, o de una llave maestra capaz de abrir todas las puertas. Obviamente, el problema sucede cuando la llave se pierde y un atacante la utiliza en beneficio propio.

Programas Salami

El principal problema de los programas salami es que son extremadamente difíciles de detectar.
Estos programas son diseñados para quedarse con los céntimos o redondeos de las operaciones financieras.
Un programa salami roba pequeñas cantidades de dinero, de forma que su acción pasa inadvertida. Aunque su efecto es especialmente grave en entornos bancarios y no en sistemas habituales.

Eavesdropping Y Packet Sniffing

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras
Vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mail entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos

Jamming O Flooding

Este tipo de ataques desactivan o saturan los recursos del sistema. Por ejemplo, un atacante puede consumir toda la memoria o espacio en disco disponible, así como enviar tanto tráfico a la red que nadie más puede utilizarla.
Muchos proveedores de Internet han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.
Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.
Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

Implementación de políticas de seguridad.

Introducción

Actualmente la seguridad informática ha tomado gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes para explorar más allá de las fronteras nacionales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

Esto ha llevado a que muchas organizaciones gubernamentales y no gubernamentales internacionales que hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.

En este sentido, las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

De acuerdo con lo anterior, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

¿Qué Son Las Políticas De Seguridad Informática (PSI)?

Una política de seguridad informática es aquella que fija los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Si bien existen algunos modelos o estructuras tipo, tiene que diseñarse "a medida" para así recoger las características propias de cada compañía.

Una buena política de seguridad corporativa debe recoger, de forma global, la estrategia para proteger y mantener la disponibilidad de los sistemas informáticos y de sus recursos. Esta visión general resulta vital para asegurar un nivel homogéneo en el grado de seguridad que quiera alcanzarse, y evitar la aparición de "agujeros negros" en determinados puntos del sistema. En definitiva, de nada sirve un excelente cortafuegos si no se encuentra

instalado un buen antivirus, o tener un avanzado software de detección de intrusos si se carece de una adecuada política de contraseñas para los usuarios.

Las áreas que contemple la política de seguridad variarán en función de cada empresa y sistema. Como mínimo deberán abordar apartados tales como: evaluación de riesgos, protección perimétrica, control de acceso a los recursos, directrices de uso de Internet y correo electrónico, antivirus, y copias de seguridad.

Otra característica importante que no debe olvidarse en las políticas de seguridad es su mantenimiento y revisión periódica. En la práctica, el crecimiento y la modificación de los sistemas de la empresa, así como la continua aparición de nuevas vulnerabilidades y amenazas, exigen que la política de seguridad corporativa sea un elemento vivo que se vaya adaptando a las necesidades que vayan surgiendo.

¿Quién es el responsable de implementar políticas de seguridad?

La Gerencia de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Junta Directiva y la Gerencia de Telecomunicaciones (cuando exista). También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

El Administrador de Sistemas es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, como por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto. El Administrador de Sistemas también es responsable de informar al Jefe de Seguridad y a sus superiores sobre toda actividad sospechosa o evento insólito. Cuando no exista un Jefe de Seguridad, el Administrador de Sistemas realizará sus funciones.

Políticas De Seguridad De Acceso Físico

Esta política tiene como objetivo vigilar y controlar los accesos o visitas al área de sistemas.

Acceso al área de sistemas

- Todo personal que quiera entrar al área de sistemas deberá registrarse y deberá mostrar tu gafete.
- El personal que acceda al área de sistemas no podrá acceder con mochilas y portafolios.
- El personal tiene prohibido entrar con dispositivos magnéticos (disquette,cds)
- El personal no podrá disponer del equipo sin una autorización previa.
- Todo personal no podrá sacar ningún dispositivo magnético sin autorización.

Políticas De Seguridad Para El Correcto Uso De Las Computadoras

Estas políticas tiene como fin el buen funcionamiento y protección de todos los equipos de computo y el buen uso de los mismos.

- Las computadoras de la Compañía sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.
- Los equipos de la Compañía sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática
- No se permite fumar, comer o beber mientras se está usando un PC.
- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).
- Deben usarse protectores contra fallas de energía eléctrica y en los servidores deben usarse fuentes de poder interrumpibles (UPS).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.
- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.
- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto y además deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.
- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.
- No está permitido llevar al sitio de trabajo computadoras portátiles (laptops) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- Los usuarios deben asumir que todo el software la Compañía está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales..
- Los usuarios no deben copiar a un medio removible (como un disquete), el software o los datos residentes en las computadoras de la Compañía, sin la aprobación previa de la gerencia.
- No pueden extraerse datos sin la aprobación previa de la gerencia. Esta política es particularmente pertinente a aquellos que usan a computadoras portátiles o están conectados a redes como Internet.
- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.
- Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos. Debe utilizarse un programa antivirus para examinar todo software que venga de afuera o inclusive de otros departamentos de la Compañía.
- No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.
- Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el Departamento de Informática.
- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.
- No deben usarse disquetes u otros medios de almacenamiento en cualquier computadora de la Compañía a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- Periódicamente debe hacerse el respaldo de los datos guardados en PCs y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de Compañía debe guardarse en otra sede, lejos del edificio.

- Los usuarios de PCs son responsables de proteger los programas y datos contra pérdida o daño. Para sistemas multiusuario y sistemas de comunicaciones, el Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).
- La información de la Compañía clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.
- No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.
- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.
- Siempre que sea posible, deba eliminarse información confidencial de los computadores y unidades de disco duro antes de que les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de una representante de la Compañía.
- No deben salirse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial de la Compañía.
- El personal que utiliza un computador portátil que contenga información confidencial de la Compañía, no debe dejarla desatendida, sobre todo cuando esté de viaje, y además esa información debe estar cifrada.

Políticas De Seguridad Para Redes

El propósito de esta política es establecer los procedimientos y los requisitos para asegurar la protección apropiada de la información al estar conectada a redes de computadoras.

Cuentas De Los Usuarios

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

- La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.
- No debe concederse una cuenta a personas que no sean empleados de la Compañía a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- Privilegios especiales, tal como la posibilidad de modificar o barrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que el Administrador de Sistemas o el Gerente de Informática determinen que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto). Si hace falta una conexión remota durante un periodo más largo, entonces se debe usar un sistema de autenticación más robusto basado contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.
- Toda cuenta queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.
- Los privilegios del sistema concedidos a los usuarios deben ser ratificados cada 6 meses. El Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior, y en particular cuando un empleado cesa en sus funciones.
- Cuando un empleado es despedido o renuncia a la Compañía, debe desactivarse su cuenta antes de que deje el cargo.

Contraseñas Y El Control De Acceso

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. No deben usarse contraseñas que son idénticas o substancialmente similares a contraseñas previamente empleadas. Siempre que posible, debe impedirse que los usuarios vuelvan a usar contraseñas anteriores.
- Las contraseñas deberán cumplir con un mínimo de 8 caracteres intercalando letras con números y símbolos.
- Nunca debe compartirse la contraseña o revelarla a otros. Él hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.
- Está prohibido el uso de contraseñas de grupo para facilitar el acceso a archivos, aplicaciones, bases de datos, computadoras, redes, y otros recursos del sistema. Esto se aplica en particular a la contraseña del administrador.
- Las contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

- Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.
- Para prevenir ataques, cuando el software del sistema lo permita, debe limitarse a 3 el número de consecutivos de intentos infructuosos de introducir la contraseña, luego de lo cual la cuenta involucrada queda suspendida y se alerta al Administrador del sistema. Si se trata de acceso remoto vía módem por discado, la sesión debe ser inmediatamente desconectada.
- Para el acceso remoto a los recursos informáticos de la Compañía, la combinación del ID de usuario y una contraseña fija no proporciona suficiente seguridad, por lo que se recomienda el uso de un sistema de autenticación más robusto basado en contraseñas dinámicas, fichas (tokens) o tarjetas inteligentes.
- Si no ha habido ninguna actividad en un terminal, PC o estación de trabajo durante un cierto periodo de tiempo, el sistema debe automáticamente borrar la pantalla y suspender la sesión. El periodo recomendado de tiempo es de 15 minutos. El re-establecimiento de la sesión requiere que el usuario proporcione se autentique mediante su contraseña (o utilice otro mecanismo, por ejemplo, tarjeta inteligente o de proximidad).
- Si el sistema de control de acceso no está funcionando propiamente, debe rechazar el acceso de los usuarios hasta que el problema se haya solucionado.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la Compañía, pudiendo ser causal de despido.
- Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.
- Los archivos de bitácora (logs) y los registros de auditoria (audit trails) que graban los eventos relevantes sobre la seguridad de los sistemas informáticos y las comunicaciones, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos tres meses. Dicho archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoria. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas.
- Los servidores de red y los equipos de comunicación (hub, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso (por ejemplo, tarjetas de proximidad).

Políticas Para El Software

- Para la instalación de algún programa se requiere que el equipo cuente con una licencia asignada o en proceso de compra, de lo contrario el software no será instalado por el personal de este departamento. Excepto en los casos de software de evaluación o gratuito.

- Para la adquisición y/o actualización de licencias (proceso de compra). Hacer una requisición especificando el número de resguardo del equipo (etiqueta ciad con código de barra, núm. entre asteriscos*numero*) y entregar una copia a cómputo de la requisición ya sellada por compras, para proceder a la instalación.

- Únicamente se harán instalaciones de software en equipos que sean del centro de computo (no se permitirá la instalación de software en equipos personales, aunque estos se estén utilizando en las labores del Centro de computo).

- El Centro de Cómputo pone a disposición del personal algunas utilerías de software, de tipo shareware, es decir el usuario las puede instalar y utilizar y en caso de que este software le sea útil, deberá adquirir la licencia correspondiente.

- La persona que tenga bajo su resguardo algún equipo de cómputo es el responsable de que el software que tenga instalado esté respaldado con una licencia de software, también esta obligado a firmar los formatos que el personal del departamento le solicite.

CONCLUSIONES

La seguridad informática es uno de los aspectos más olvidados en la mayoría de las empresas o organizaciones, todavía no tienen idea de los riesgos que puede causar la falta de seguridad en sus sistemas informaticos, hoy en día con los avances tecnológicos y el mayor auge del Internet La seguridad informática ya es una necesidad, no un capricho ni un lujo para cualquier empresa o organización.

La seguridad no puede ser vista como un producto que se instala una vez y se deja olvidado, sino como una necesidad primordial. La seguridad debe cumplir con un proceso de monitoreo, verificación, y actualización. La única manera de evitar ser una víctima más de los ataques externos a través de redes globales, tales como Internet, es el conocimiento de las vulnerabilidades a que se está expuesto y el emprendimiento de acciones y estrategias para minimizar los riesgos

Debemos hacer conciencia que La seguridad requiere también de la participación de todos, usuarios, programadores, administradores cumpliendo con las normas o políticas de seguridad que estén establecidas para brindar un ambiente seguro en la organización.

El crecimiento de las redes y la consecuente conectividad entre sistemas representa nuevas oportunidades, no sólo positivas, sino también negativas al facilitar por ejemplo los accesos no autorizados y al reducir las facilidades de control centralizado y especializado de los sistemas de información.

Las amenazas a la información pueden ser de origen diverso, con los tiempos se van generando nuevas formas de daño a ella. Hay amenazas de origen natural (terremotos, tormentas, etc.), origen humano (robo, sabotaje, chantaje, entre otros) y origen técnico (fallas, alta tensión) Esto lleva a que la función de definir los planes a seguir en cuestión de seguridad debe de tomarse en cuenta la seguridad física y la lógica.

Al hablar de seguridad hay que involucrar muchos aspectos que no solo están relacionados con herramientas tecnológicas, no solo implica una solución de hardware y software, también involucra a los tomadores de decisiones, que son finalmente quienes deciden las inversiones, ellos deben comprender claramente la problemática para destinar los recursos necesarios para garantizar la confiabilidad, disponibilidad e integridad de los datos.

La puesta en marcha de los planes o métodos de seguridad a seguir es responsabilidad del encargado de la seguridad, pero también debe existir un compromiso de parte de los usuarios de sistema de información, ejecutivos y todas las personas que de alguna u otra forma ayudan a que este sistema satisfaga a los requerimientos que se ve enfrentado, manteniendo sobretodo la integridad y confidencialidad de la información

La seguridad informática es un conjunto de planes y estrategias enfocadas a reducir los riesgos y tiene como objetivo definir, implementar y controlar los mecanismos de seguridad para proteger a la información de las diversas amenazas a las que se ve enfrentada.

El objetivo o propósito de esta tesina sobre seguridad informática es tener en cuenta las diferentes amenazas que pueden estar expuestos los sistemas de información y también las formas de contrarrestarlas aplicando las medidas de seguridad convenientes

BIBLIOGRAFIA

1) Delitos Informaticos
http://delitosinformaticos.com/seguridad.shtml

2) Seguridad En La Red
http://seguridad.internautas.org/puertos.php

3) Seguridad Informática
http://www.hispasec.com/

4) guía de seguridad
http://www.sedisi.es/05_Estudios/guia01.htm

5) Seguridad Física
http://cfbsoft.iespana.es/cfbsoft_es/seguridad/fisica.htm

6) Seguridad Física En General
http://www.colpos.mx/cominf/mmsegurid.htm

7) Riesgos Ambientales Y Humanos
http://www.a.potlatch.net/main/espanol/et/ete01a.htm

8) Seguridad Informática
http://www.svetlian.com/Seguridad/

9) Seguridad Física Y Lógica
http://www.internet-solutions.com

10) Seguridad Lógica
http://www.eduardoleyton.com/SLogica.html

11) Seguridad Lógica
http://www.sgi.es/que_hacemos/seguridad_logica.htm

12) Seguridad En Redes
http://www.criptonomicon.com/links/check.html

13) Escaneo De Puertos
http://grc.com/

14) Protección De Puertos

http://www.nicolaso.com/seguridad_pages/puertos.htm

15) Seguridad Corporativa
http://www.seguridadcorporativa.org/seguridadcorporativa/seguridadinformatica.html

16) Bloqueo De Puertos
http://seguridad.internautas.org/bloqueo.php

17) Seguridad De Sistemas
http://www.infodynamics.com.uy/seguridad.asp

18) Virus
http://www.virusprot.com/

19) Ataques
http://www.supercable.es/~kernel/intrusion.htm

20) Seguridad Informática
http://www.obconsultores.com/SegInf/intro.htm

21) Hackers
http://www.hackhispano.com/

22) Sistemas De Seguridad
http://www.mundovivo.com/

23) Antivirus
http://www.zonavirus.com/Detalle_Noticia.asp?noticia=451&enlazado=248

24) Antivirus
http://www.udec.cl/~sscheel/pagina%20virus/Antivirus.htm

25) Riesgos Ambientales
http://www.sc.ehu.es/scwreall/documentos/plan-seg-fisica.html

26) Amenazas A La Información
http://www.iec.csic.es/criptonomicon/seguridad/amenazas.html

27) Protección De Datos
http://www.itson.mx/dii/jgaxiola/cursos/admon_tecnologia/seguridad_de_los_datos.htm

28) Seguridad En Redes
http://www.ucpr.edu.co/auditores/boletin/boletin_8d/index.htm

29) Seguridad
http://www.eumed.net/cursecon/ecoinet/seguridad/index.htm

30) Sistemas Biométricos
http://www.globalcard2000.com/es/biometria/index.htm

31) Biometría
http://www.infovox.com.co/Biometria.htm

32) Biometría
The Biometric Consortium.

33) Hackers Y Crackers
http://www.duiops.net/hacking/hackvsc.htm

34) Software De Análisis
http://www.neotec.com.pa/ITSecurity/biologon.htm

35) Firewall
http://www.penta2.ufrgs.br/gereseg/unlp/12tema2.htm

36) Firewall
www.desarrolloweb.com/articulos/513.php

37) Niveles De Seguridad
http://www.tuguialegal.com/docseguridad1.htm

38) Encriptación
http://www.terra.es/tecnologia/articulo/html/tec8857.htm

39) Encriptación
http://intranet.logiconline.org.ve/articulos/encriptacion.html

40) Ingeniería Social
http://www.vsantivirus.com/lz-ingenieria.htm

41) Políticas De Seguridad
http://www.hospitalsanjusto.org.ar/politicaprivacidad.htm

42) Políticas De Seguridad
http://www.uady.mx/sitios/seguridad/documentos/capitulo2.htm#art5

43) Agujeros De Seguridad
http://www.rebelion.org/cibercensura/mostazo170103.htm

44) Tipos De Virus
http://www.obconsultores.com/VirInf/index.htm

45) Mentes Inquietas
http://www.mentes.org/html/

46) Backup
http://www.ussg.iu.edu/usail/index/backup.html

47) Seguridad En General
http://www.pvv.ntnu.no/cert/security.html

48) Control De Accesos
http://acceso.rhon.itam.mx/solicitud.html

49) Seguridad De Sistemas
http://www.seguridadysistemas.com/index.php

50) Amenazas Humanas
http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_2122.html

51) Técnicas De Control Interno
Http://Www.Cortedecuentas.Gob.Sv/Cap%C3%Adtulo4.Htm

52) Libro Electrónico
Amenazas A La Información.
Anónimo.

53) Libro Electrónico
Manual De Seguridad.
Anónimo

54) Libro Electrónico
Seguridad Informática
Anónimo.

55) Libro Electrónico
Gestión Global De La Seguridad
Ricardo Cañizares Sales

56) Libro Electrónico
Seguridad En Los Sistemas

M. Farias Elinos.

57) CD ROM
Utilidades Forenses
Ing. Miguel Ángel Álvarez

58) Informática Forense
Apuntes Del Diplomado
Ing. Miguel Ángel Álvarez