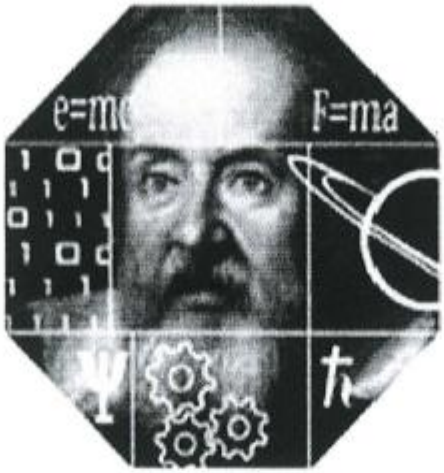
JORGE WILLIAM BARRIOS HERNÁNDEZ



UNIVERSIDAD

Galileo

Guatemala, C. A.

"ESQUEMAS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN"

LICENCIATURA EN ADMINISTRACIÓN DE SISTEMAS DE INFORMACIÓN

FACULTAD DE INGENIERÍA DE SISTEMAS, INFORMÁTICA Y CIENCIAS DE LA COMPUTACIÓN

GUATEMALA, 2012

UNIVERSIDAD
Galileo

Guatemala, 31 de agosto del 2012

Señor
Jorge William Barrios Hernández
Presente

Estimado Señor Barrios:

En base a la Resolución No. 7247-III-2012 del Consejo Directivo de esta Universidad, de fecha 30 de agosto del 2012, en donde se le reconoce como autor del trabajo de tesis titulado ESQUEMAS DE SEGURIDAD EN SISTEMAS DE INFORMACION, y de haber obtenido el dictamen del Asesor específico, Lic. Hans Bandow, se autoriza la publicación del mismo.

Aprovecho la oportunidad para felicitarlo por el magnífico trabajo realizado, el cual es de indiscutible beneficio para el desarrollo de las Ciencias de la Computación en Guatemala.

Atentamente,

FACULTAD DE INGENIERIA DE SISTEMAS
INFORMATICA Y CIENCIAS DE LA COMPUTACION

Ing. José Eduardo Suger Castillo
Decano
FISICC

Ing. Rodrigo Baessa
Vice-Decano FISICC

bder/

UNIVERSIDAD Galileo

MEMORANDUM

A: Jorge William Barrios Hernández
Estudiante Licenciatura en Administración de Sistemas de Información
Universidad Galileo

DE: MA. Jorge Francisco Retolaza
Secretario General
Universidad Galileo

ASUNTO: Reconocimiento de autoría de Tesis

FECHA: 30 de agosto de 2012

A continuación me permito transcribirle la resolución del Consejo Directivo en su sesión del seis de marzo del dos mil doce, con relación al reconocimiento de autoría de tesis.

RESOLUCION 7247-III-2012.- El Consejo Directivo conoció la solicitud presentada por el Lic. Manuel Monroy, Director de la carrera de Licenciatura en Administración de Sistemas de Información, en donde solicita que al alumno Jorge William Barrios Hernández, carné I589246, le sea reconocida la autoría de la tesis denominada "Esquemas de Seguridad en Sistemas de Información", la cual fue elaborada conjuntamente con los estudiantes Gustavo Gerardo Guillen Barillas, carné I590371 y Alvaro Roberto Guillen Barillas, carné I184078, graduados de la Universidad Francisco Marroquín en noviembre del 2000 y cuya tesis fue publicada.

Después de analizar la solicitud planteada, la documentación presentada por el alumno Jorge William Barrios Hernández y la autorización de elaboración de tesis que obra dentro del expediente, el Consejo Directivo resuelve reconocerlo también como autor de la tesis "Esquemas de Seguridad en Sistemas de Información" y en consecuencia aceptarla como requisito de graduación.

Atentamente,

Lic. Jorge Retolaza
Secretario General

Acta 218-2012

C. Archivo
Rectoría
Vicerrector
Vicerrector Administrativo
Expediente alumno
Lic. Manuel Monroy – Director L.A.S.I

UNIVERSIDAD FRANCISCO MARROQUIN

FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION

Guatemala, 16 de agosto de 2000

Señores
Alvaro Roberto Guillén Barillas y
Gustavo Gerardo Guillén Barillas
Presente

Estimados señores Guillén Barillas:

Tengo mucho gusto en informarles que, después de haber revisado su trabajo de Tesis, cuyo título es **"Esquemas de Seguridad en Sistemas de Información"** y de haber obtenido el dictamen del asesor específico, autorizo la publicación del mismo.

Aprovecho la oportunidad para felicitarlos por el magnífico trabajo realizado, el cual es de indiscutible beneficio para el desarrollo de las Ciencias de Computación en Guatemala.

Atentamente,

FACULTAD DE INGENIERIA DE SISTEMAS,
INFORMATICA Y CIENCIAS DE LA COMPUTACION

Dr. Eduardo Suger C.
Decano FISICC

ESC/cdcc.-

Guatemala, 19 de julio del 2,000

Doctor
Eduardo Suger
Decano de FISICC
Universidad Francisco Marroquín
Presente

Estimado Dr. Suger

Por medio de la presente deseo hacer de su conocimiento que he revisado el trabajo de Tesis denominado "Esquemas de seguridad en sistemas de información" elaborado por los señores Alvaro Guillén, Jorge Barrios y Gustavo Guillén.

El trabajo a mi juicio cumple con los requisitos establecidos para optar al grado académico respectivo, y como asesor de la tesis, doy mi aprobación al trabajo realizado, dejando a su criterio la aprobación final del mismo.

Sin otro particular, me suscribo de usted

Atentamente,

Lic. Hans Bandow

UNIVERSIDAD FRANCISCO MARROQUIN

APARTADO POSTAL 1-32 - A
01008 GUATEMALA, C. A.
TELS (502-2) 346886 / 95
FAX (502-2) 346890

Guatemala,
7 de agosto del 2000

Doctor
Eduardo Suger Cofiño
Decano de la Facultad de Ingeniería de
Sistemas, Informática y Ciencias de la
Computación

Doctor Suger:

Por medio de la presente me permito informarle que lei la tesis de los alumnos GUSTAVO GERARDO GUILLÉN BARILLAS, ALVARO ROBERTO GUILLÉN BARILLAS Y JORGE WILLIAM BARRIOS HERNÁNDEZ titulada **ESQUEMAS DE SEGURIDAD EN SISTEMAS DE INFORMACIÓN** , asesorada por el licenciado Karl Hans Bandow Andrade.

Después de haber hecho las correcciones y recomendaciones pertinentes, me es grato comunicarle, en mi calidad de revisora de redacción, estilo y ortografia, que dicha tesis llena los requisitos que exige la Univesidad .

Me suscribo del Señor Decano, como su atenta servidora.

Licda. Marta Judith Palma de Pineda.

c. c.: Archivo

INTRODUCCIÓN

Seguridad y el deseo de sobrevivir, son instintos básicos que son evidentes en todos los aspectos de la vida. Las organizaciones en General, exhiben y practican estos instintos con diferentes grados de éxito.

Históricamente, las organizaciones han estado conscientes de su propia seguridad, por lo que han ido construyéndola y mejorándola cada vez más. Sin embargo, el crecimiento competitivo en el ambiente del negocio en general, pone a las organizaciones en una situación de generar un esfuerzo mayor por mantener e incrementar su participación en el mercado.

Por lo tanto, un balance efectivo entre seguridad y riesgo es fundamental para alcanzar el éxito. La seguridad de informática es un problema de la organización y no un problema técnico.

Los avances tecnológicos han hecho que la información sea más disponible y por lo tanto más vulnerable a acceso no autorizados y a ser manipulada. Debilidades en los procedimientos de control de los sistemas pueden permitir la infracción de integridad de la información.

La información es un activo estratégico para todas las organizaciones, por lo tanto la alteración no autorizada y/o destrucción de la información puede resultar en un daño grave para el negocio y la reputación de la organización.

Para asegurar los niveles básicos de confidencialidad, integridad y disponibilidad de la información, se deben definir esquemas de seguridad en los sistemas de información

CAPÍTULO 1

1. Qué es un sistema de información

En el sentido más amplio, un sistema es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común. La sociedad está rodeada de sistemas. Por ejemplo, cualquier persona experimenta sensaciones físicas gracias a un complejo sistema nervioso formado por el cerebro, la médula espinal, los nervios y las células sensoriales especializadas que se encuentran debajo de la piel; estos elementos funcionan en conjunto para hacer que el sujeto experimente sensaciones de frio, calor, comezón y otros.

Todo sistema depende en mayor o menor medida, de una entidad abstracta denominada sistema de información. Este sistema es el medio por el cual los datos fluyen de una persona o departamento a otros y puede ser cualquier cosa, desde la comunicación interna entre los diferentes componentes de la organización y líneas telefónicas hasta sistemas que generan reportes y consultas para usuarios.

1.1 Características importantes de los sistemas

La finalidad de un sistema es la razón de su existencia. Para alcanzar sus objetivos, los sistemas interaccionan con su medio ambiente, el cual está formado por todos los objetos que se encuentran fuera de las fronteras del sistema. Los sistemas que interactuan con su medio ambiente (reciben entradas y producen salidas) se denominan sistemas abiertos. En contraste, aquellos que no interactuan con su medio ambiente se conocen como sistemas cerrados.

Todos los sistemas tienen niveles aceptables de desempeño, denominados estándares contra los que se debe comparar el nivel de desempeño actual de nuestros sistemas, a fin de realizar ajustes si fuera necesario.

1.2 La información y su importancia dentro de una organización

El término información contiene como tal una gran gama de acepciones, literalmente conduce a palabras como noticias, datos, conocimientos y otros. La información en un concepto central designa no sólo los conocimientos que los hombres se transmiten entre sí, sino ante todo, una de las propiedades fundamentales del mundo objetivo que se haya vinculada a la presencia en este tipo especial de procesos denominados de información.

Procesos de información son, por ejemplo, la comunicación de los hombres entre sí, la labor de cualquier sistema de regulación automática, la transmisión hereditaria de los caracteres de padres a hijos, el conocimientos del mundo por el cerebro humano.

La información en la organización está formada por toda aquella información que circula a través de tecnologías como faxes, internet, intranets, extranets, correos electrónicos y otros. A este tipo de información se le conoce comúnmente como información digitalizada.

Toda la información que corre a lo largo de los procesos de la organización es la que sirve para cerrar un negocio, ofrecer algún servicio al cliente, tomar decisiones y muchos usos más, por lo que la información es un activo muy valioso para la organización.

Una manera de medir si la información es clave en la organización es: Estimar como la información facilita los intercambios con los clientes y los proveedores así como en el mismo interior de la organización.

Para disponer de la mejor información hay que considerar los siguientes aspectos:

Se pueden generar más beneficios

Se pueden reducir costos

Se puede vender la información de que dispone la organización como un producto derivado de la misma actividad?

1.3 Como manejar la información

A medida que crece el volumen de la información a manejar, aumenta la necesidad de disponer de una *Tecnología de la Información* que soporte dinámica y eficazmente el funcionamiento normal de las distintas áreas o departamentos que la constituyen y que protejan la información ante cualquier alteración no autorizada.

En la actualidad, las organizaciones cuentan con sus propios sistemas de información los cuales interactúan en una red de computadoras. A continuación se hace una descripción de las redes locales (LAN) y redes de área ampliada (WAN) y sus componentes para luego ver en los siguientes capítulos como aplicarles esquemas de seguridad a fin de tener información confiable y oportuna.

1.4 Red de área local (LAN)

Una Red de Area Local (LAN) es una red de computadoras que ofrece servicios de transporte de información entre oficinas dentro de un edificio o grupo de edificios, es decir, en distancias cortas.

Las facilidades de una red local permiten que las estaciones de trabajo se vinculen a Servidores de Archivo, amplias bases de datos y otras estaciones de trabajo en toda la organización.

La capacidad de crecimiento de las Redes de Área Local, permiten más información e intercambio de datos en la organización y conducen a aplicaciones tecnológicas más complejas.

La madurez de las interfases para usuarios en particular, el aumento de interfases gráficas y la integración de datos, textos, voz e imagen hace que la tecnología sea más útil para el hombre común. En la figura 1.1 se muestra un esquema de una red LAN.

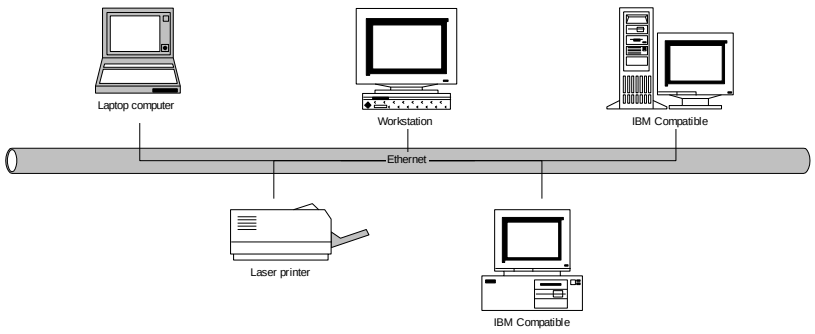


Figura 1.1.

1.5 Red de área ampliada (WAN)

Una Red de Área Ampliada (WAN) es una red que ofrece servicios de transporte de información entre zonas geográficamente distantes. Es el método más efectivo de transmisión de información entre edificios o departamentos distantes entre sí. Esta forma de comunicación aporta, como nota diferencial con respecto a las Redes de Área Local (Redes Informáticas) o las Redes de Área Metropolitana (MAN), el ámbito geográfico que puede cubrir, el cual es considerablemente muy amplio.

La tecnología WAN ha evolucionado rápidamente en los últimos años, especialmente, a medida que las empresas de telecomunicaciones han reemplazado sus viejas redes de cobre con redes más rápidas y fiables de fibra óptica, dado que las redes públicas de datos son el soporte principal para construir una red WAN.

Cuando una organización se plantea el uso de una Red de Área Ampliada, persigue una serie de objetivos:

Servicios integrados a la medida de sus necesidades (integración de voz, datos e imagen, servicios de valor añadido, etc.).

Integración virtual de todos los entornos y dependencias, sin importar donde se encuentren geográficamente situados.

Optimización de los costos de los servicios de telecomunicación.

Flexibilidad en cuanto a disponibilidad de herramientas y métodos de explotación, que le permitan ajustar la configuración de la red, así como variar el perfil y administración de sus servicios.

Mínimo coste de la inversión en equipos, servicios y gestión de la red.

Alta disponibilidad y calidad de la red, soporte de los servicios.

Garantía de evolución tecnológica.

Componentes de una Red Informática

A continuación se define una serie de equipos (hardware) y programas (software) que constituyen componentes de una red informática.

1.6 Componentes de Hardware

1.6.1 Servidores

Se definen como equipos de procesamiento, de capacidad multiusuario, con memoria compartida, que ofrecen servicios apropiados de cómputo, conectividad y acceso a Base de Datos. Este concepto plantea que existen varios tipos de Servidores y que éstos, se clasifican por el tipo de servicio que proveen, como son algunos ejemplos:

Servidores de Aplicaciones. Aquellos que proveen acceso a las aplicaciones que procesan datos.

Servidores de Datos. Proveen acceso a los datos, textos, voz, imagen y gráficos.

Servidor de Comunicaciones. Son aquellos que proveen acceso a servicios de comunicación externos.

Servidores de Impresión. Aquellos que proveen acceso a equipo de impresoras.

1.6.2 Estaciones de trabajo de red

Son aquellas estaciones de trabajo (computadoras personal o portátiles) que se conectan a la Red, llevan adelante tareas dentro del proceso cooperativo de la organización, demanda y obtiene servicios de procesamiento, de acceso a datos, impresiones y/o a quien envía determinada información o tarea, como envío o recepción de faxes.

1.6.3 Estaciones de trabajo gráfico

Son estaciones de trabajo que llevan adelante tareas muy especializadas y demandan de una configuración especial del equipo, por ejemplo: Sistemas Multimedia, Diseño Asistido por Computadora, Sistemas de Información Geográfica.

Muchas veces estos equipos operan dentro de una red Informática y constituyen terminales de trabajo en el marco de la red. En la actualidad, ya se dispone de Sistemas de Información Multimedia y de Sistemas de Gestión de Bases de Datos Gráficas y Multimedia, que permiten el establecimiento de Estaciones Gráficas en Red.

1.6.4 Tarjetas de interfase o adaptadores de red

Es un dispositivo digital (a modo de tarjeta o pastilla), que convierte el flujo serial de alto poder de datos del cable de la red a un flujo de datos paralelos.

1.6.5 Cableado

El Cableado es el medio físico por el que transcurren las señales digitales. Está compuesto por varios elementos, entre los que se tienen:

- Cableado
- Conectores
- Concentradores
- Racks
- Switches
- Ruteadores
- Bridges
- Gateways

Cableado

Se define como el conducto por el cual se transmite las señales eléctricas o luminosas, pueden ser de cobre (las más comunes) o fibra óptica (para trasmitir señales luminosas).

Conectores

Son dispositivos físicos de empalme entre cables, (para el uso de redes de tipo Bus), el cable y la tarjeta o adaptador de red, el cable y los concentradores, el Swiching, Routers o Bridges, son de diversos tipos siendo los más comunes los BNC, RJ-45 y AUI.

Concentradores

Los concentradores o hubs (centrales de cableado), se conectan a grupos dentro de los nodos de redes, aislando cada nodo de cualquier problema. Los grupos varían según el concentrador, pudiendo ser de 8, 12, 16, 32 puertos del tipo RJ 45, más una salida AUI y BNC. Cada uno de estos concentradores se encadenan a otros en la red, agregando capacidad hub por hub, según el criterio de:

Bus

Consiste en un único cable de transmisión al cual se unen los nodos que integran la red. Es también conocida como línea "*multi-drop*" y regularmente se utiliza en redes "Ethernet"

Cascada

Esta sub-categoría, está limitada a la conexión de cinco concentradores, utilizando un puerto de tipo RJ 45 y/o de una calidad de fibra óptica, con un dispositivo llamado transceiver, que se incorpora al concentrador.

Apilamiento

Esta sub-categoría, permite conectar varios concentradores en pilas a través del puerto AUI o de la implantación de transceiver. Este apilamiento varía y permite concentrar una cantidad muy grande de grupos de nodos.

Rack

Para la estructuración de una red se implementa un Rack, que en realidad no es más que un "Mueble", el cual permite agrupar en un determinado número de concentradores o Hubs. A este "mueble", se adiciona salidas para el cableado.

Switching

La tecnología de switching o de "interruptores", es hoy en día la opción tecnológica más promovida e interesante, pues los switches constituyen verdaderas centrales de comunicaciones de una red estándar, en la cual cada nodo sigue un esquema de control de acceso a medios (MAC), como Ethernet o Token Ring que permita compartir los tiempos en cable.

Bajo el principio de cuanto más nodos haya en una LAN, será menor la cantidad de tiempo que va a necesitar para las transmisiones, un switch aísla y cataliza los datos, de modo que cada nodo tiene acceso ilimitado al cable.

El switch es la tecnología más sencilla y económica para mejorar el desempeño de una red muy ocupada. Existen muchos tipos de switches, desde aquellos que unen a algunos segmentos de red a los Inter redes, que integran redes Locales y Remotas a grandes distancias, estas últimas prestan facilidades combinadas de Routers, Gateways y Bridges.

Ruteadores

Los Servidores de Comunicaciones vienen de muchas formas y en diferentes roles funcionales, aunque de manera fundamental contienen las redes de Alta Velocidad en

área local de 10 a 100 Mbps, muy por encima de la Milla (1,7 Km). Los Servidores de Comunicaciones que encadenan, utilizan técnicas sofisticadas de inspección de paquetes para enrutar el tráfico hasta su destino.

Un ruteador está programado para leer una gran cantidad de protocolos, siendo los principales:

IPX/SPX

TCP/IP

AppleTalk

Estos protocolos de enrutamiento incluyen el Protocolo de Enrutamiento de Información (RIP), que primero abre el camino más corto, y los que son utilizados por las redes basadas en TCP/IP. El protocolo Interior de Compuerta de Enrutamiento, el protocolo de Encadenamiento de Servicios Netware, son los más novedosos.

La Nueva generación de Ruteadores, descansa en la combinación con los Swiching, los Bridges y/o en una PC dedicada, con un Sistema Operativo de Multiprogramación: UNIX, Novell, Windows NT, OS/2X; una tarjeta Multi puerto y Software con capacidad Multiprotocolo.

Bridges

Es un dispositivo digital (en las versiones modernas es solo software), que conecta dos redes de igual tipo.

Gateways

Tal como se muestra en la figura 1.2 un Gateway es un dispositivo digital que conecta dos tipos diferentes de redes de comunicaciones. Realiza conversión de protocolos de una red a otra.

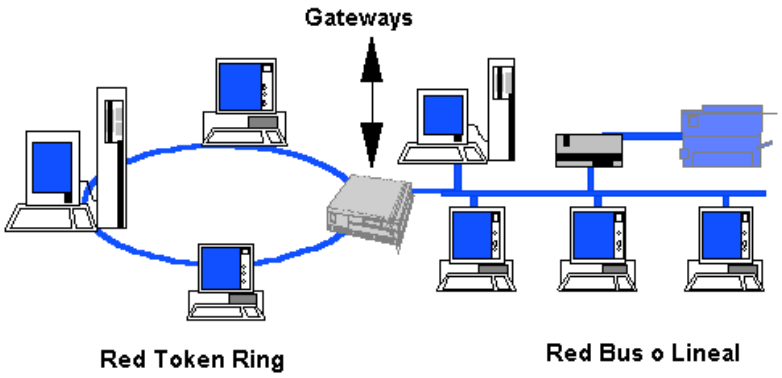


Figura 1.2

Integradores

En la actualidad todas las tecnologías expresadas anteriormente, están operando sobre una sola plataforma llamada “Integradores”.

Adaptadores de una red inalámbrica

En una Red Inalámbrica, también se usan adaptadores (Tarjetas) de Red, que instaladas sobre la PC Cliente, permiten conectarse a la frecuencia en que está transmitiendo el Servidor Central, por lo general a través de una antena. Dependiendo de la Potencia del Transmisor del Servidor Central (o Troncal), se determina el área de acceso o celda, en la cual pueden operar las estaciones clientes, incluyendo las PC Móviles (Notebooks). En la figura 1.3 se aprecia la estructura de un modelo de ded Informática, que incorpora

Switching, concentradores agrupados en un rack y concentradores departamentales.

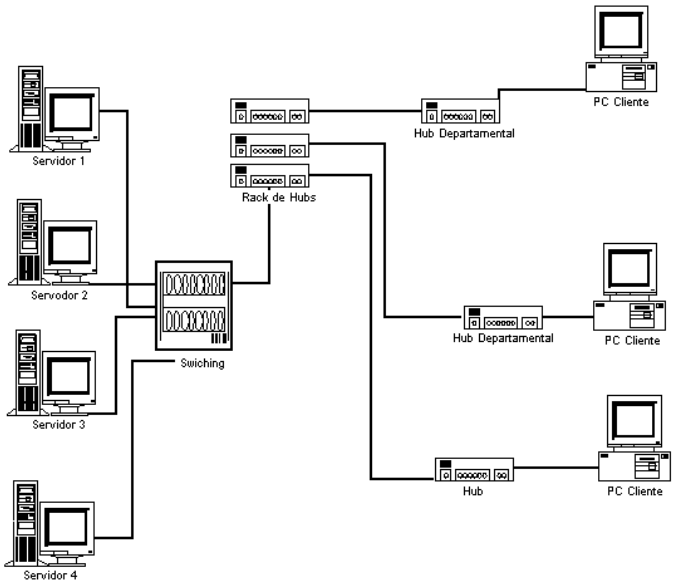


Figura 1.3

Componentes de Software

En este punto se analizan los elementos complementarios a los dispositivos físicos, se refiere al software, que permite la interconexión de los datos y aplicaciones.

1.7 Sistema Operativo de Red

El Sistema Operativo de Redes (Net Operating Systen - NOS), es el software que contiene todos los elementos básicos para compartir recursos. Algunos productos separan las funciones de cliente de las de servidor. Pero una PC puede jugar ambos roles.

El Sistema Operativo de Red afina el servidor, al administrar su memoria, y aloja las tareas a través de múltiples procesadores, con lo cual proporciona capacidad para crecer.

Entre las características que debe ofrecer un Sistema Operativo de Red se tiene:

1.7.1 Conectividad

El NOS debe comunicarse de manera simultánea, a través de protocolos múltiples como Decena, IPX/SPX, NetBEUI y TCP/IP.

1.7.2 Escalabilidad

El NOS debe garantizar el crecimiento y consistencia de la operatividad de la red, con la misma eficiencia de partir de una red de 5 usuarios hasta de 1000 usuarios o más.

La figura 1.4 muestra gráficamente la escalabilidad de un sistema.

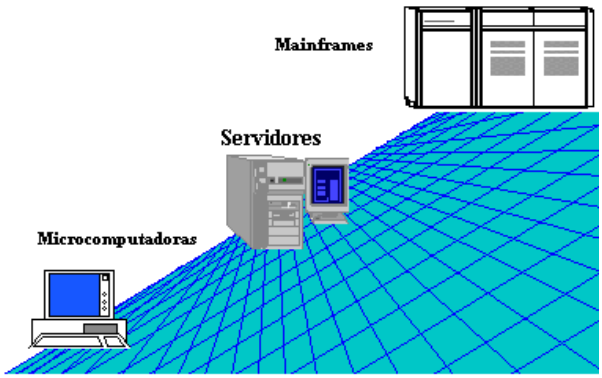


Figura 1.4

1.7.3 Arquitectura modular

El NOS debe permitir agregar hardware y software en forma sencilla. Los servicios adicionales de redes incluyen telefonía, respaldo, correo electrónico, conectividad, acceso remoto y deben ser fáciles de instalar y configurar a través de la red. La figura 5.1 muestra un esquema de arquitectura modular.

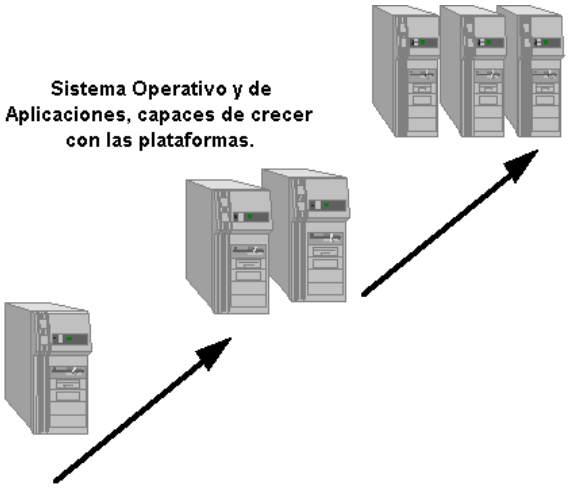


Figura 1.5

1.7.4 Diversidad

El NOS debe darle servicio a los requerimientos de las estaciones de trabajo en diferentes plataformas: MacOs, Windows, OS/2 y Sistemas UNIX, deben conectarse fácilmente a la Red. La figura 1.6 muestra una integración de varias plataformas.

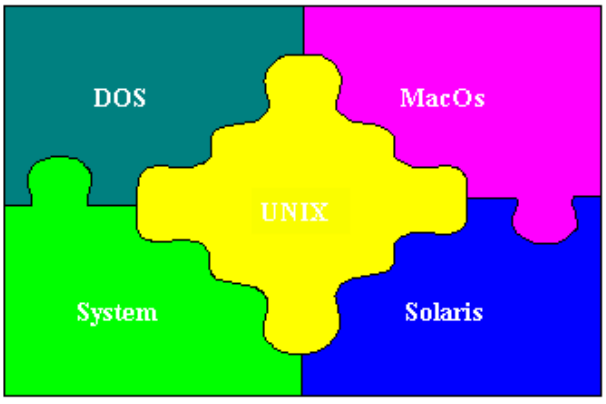


Figura 1.6

1.7.5 Simplicidad

El NOS debe ser fácil de instalar y reconfigurar, se deja ejecutar el proceso de apagado y encendido y se instala desde un CD ROM. Además debe detectar el hardware del servidor. Para una administración sencilla, debe tener una interfase gráfica de usuario que permita visualizar, seleccionar, arrastrar y soltar funciones. También debe permitir agregar usuarios y grupos fácilmente al permitirles el derecho de acceso a los servidores.

1.7.6 Desempeño

El NOS debe proporcionar muchas características principales, para darle servicio a los requerimientos de archivos y poder correr aplicaciones cliente / servidor, que incluya administración avanzada de memoria, las técnicas para multitarea y el multiprocesamiento simétrico.

1.7.7 Compartición de recursos confiabilidad

El NOS debe permitir compartir recursos como impresoras, modem, aplicaciones y otros a través de la Red. La seguridad completa, en realidad, incluye contraseñas para archivos, usuarios y grupos, así como un sistema para detección de intrusos.

1.7.8 Sistema de administración de red

Con las redes creciendo en tamaño y complejidad, los administradores de redes necesitan una manera de controlar y supervisar mejor una red que abarque toda la organización. Tanto las compañías proveedoras de NOS, como terceros, están desarrollando productos

de gestión de redes, entre las principales características de estos sistemas de control, almacenados en su Base de Datos de Administración de la Red, se tienen:

- Listado, descripción y evaluación de operación de los dispositivos de la Red: Concentradores, cableado, servidores, UPS.
- Control de operaciones con los dispositivos, gestión de colas en la red.
- Organización, creación, derechos de acceso y administración de listas de usuarios.
- Control de errores más comunes en la red.
- Estadísticas del servidor y del servicio.
- Supervisión de seguridad de usuarios, datos y dispositivos.

CAPÍTULO 2

2. Seguridad como un elemento estratégico para la organización

2.1 Definición de seguridad

Seguridad es la protección de la información, programas y componentes físicos de informática en los siguientes términos: Confidencialidad, Integridad y Disponibilidad.

Aclaración de algunos términos:

Información y activos de computación, cubre cualquier tipo de dato, software comercial, sistemas de información, redes de trabajo, incluyendo cualquier documento relacionado a Informática dentro de la empresa.

ISO 7498-2 (1989), refiriéndose al modelo OSI, define los términos de integridad, disponibilidad e integridad de la siguiente forma:

Integridad: Es la propiedad que define que la información no deber ser alterada o destruida sin autorización.

Disponibilidad: Es la propiedad que define que la información esté accesible y utilizable en demanda de una entidad autorizada.

Confidencialidad: Es la propiedad que define que la información no deberá estar disponible o revelada a individuos no autorizados, entidades o procesos.

2.2 Objetivo de seguridad en informática

Los esfuerzos de seguridad están dirigidos a asegurar la continuidad del negocio y minimizar los daños al negocio a través de la prevención o minimización de incidentes.

El esfuerzo envuelto en la seguridad de la informática está determinado por la probabilidad de que un desastre ocurra y el posible impacto al negocio.

2.3 Propuesta de seguridad en informática

Proporcionar un juego de controles de seguridad para garantizar los niveles básicos de confidencialidad, integridad y disponibilidad de la información, programas y componentes físicos de informática, así como la prevención de riesgos y medidas para minimizar los efectos causados ante un desastre.

2.4 Buenas prácticas de seguridad

2.4.1 Plan de recuperación ante un desastre

Toda organización que basa sus operaciones en un sistema de informática, debe tener conocimiento que cualquier falla es potencialmente seria. Hay varias medidas de protección que se puedan tomar, pero la más importante de ella, es tener un plan de recuperación ante un desastre, para no poner en riesgo la continuidad de sus operaciones.

2.4.2 Servicio de calidad

Los servicios de informática de la organización, hacen una contribución muy crítica a la calidad del negocio, por lo que se debe garantizar la continuidad de las operaciones

poniendo en práctica el plan de recuperación u otras medidas de seguridad, de tal forma que el incidente sea para el usuario lo más transparente posible.

2.4.3 Creando y manteniendo un nivel competitivo

Con la creación de nuevos productos, nuevos servicios y la constante optimización de los procesos, se provee a la organización, nuevas herramientas que le permiten alcanzar niveles de rapidez y eficiencia en la atención a los clientes.

2.4.4 Confianza en el sistema de informática

Proporcionarle al usuario la certeza de poder ejecutar las operaciones en cualquier momento que se requiera y evitar al máximo tener que decir frases como: “Lo siento no puedo hacerlo, pues no tenemos sistema en este momento”.

2.4.5 Cumplir con la legislación y las leyes

La organización debe asegurarse de no incurrir en delitos por fallas en la seguridad o en las operaciones de su sistema de informática. Por ejemplo piratería industrial, derechos de autor.

2.4.6 Minimizar el costo de seguros

La organización debe identificar los riesgos más altos a los que está expuesta, pues las aseguradoras cobran grandes cantidades de dinero, por altos riesgos bien identificados.

2.4.7 Protección a los usuarios

Coordinar políticas de seguridad industrial para la manipulación de los componentes del sistema de informática, para proteger a los usuarios de posibles fallas.

2.4.8 Auditoría de sistemas

La auditoría informática es una función cuya misión es garantizar la seguridad, eficacia y rentabilidad del Sistema de Información. Esto es de gran importancia y se ve amenazada por factores intrínsecos de alto riesgo ya que, fallas en los sistemas informáticos pueden generar graves daños, materializados en pérdidas de patrimonio y operatividad, distorsiones en el servicio, inconsistencia en la gestión y deterioro de la imagen.

Los objetivos de una auditoría de sistemas son: implementar los controles necesarios en el ámbito global de los sistemas y establecer las especificaciones necesarias para la verificación y adecuación de éstos, de modo tal que se asegure la exactitud, seguridad e integridad de los sistemas y sus resultados.

Las fases de una auditoría son:

- Diagnóstico de la situación actual
- Identificación de necesidades para realizar la auditoría y establecer el plan
- Capacitación del personal en los métodos a implementar
- Formulación del plan de implementación y desarrollo de las actividades de auditoría informática

La realización de una auditoría implica una estimación de:

- La efectividad en términos de costo de los nuevos sistemas propuestos
- La eficiencia de los sistemas
- Las provisiones de respaldo que existen en el lugar
- La seguridad suministrada
- La integridad de la documentación
- La factibilidad de los planes de implantación
- Auditabilidad

La auditabilidad provee facilidad relativa en examinar, verificar o demostrar un sistema. Debe ser posible que esta determinación la puedan realizar personas independientes al sistema. En el caso específico de un sistema de información, se debe determinar que el sistema esté intentando usarse, así como está siendo usado, que la aplicación del sistema está conforme a los estándares y que la información contenida en la aplicación del sistema está conforme a lo esperado (ejemplo: exacto, completo, en conformidad con el ambiente).

Para que un sistema sea auditable, debe satisfacer las pruebas de "contabilidad" y "visibilidad". La primera debe posibilitar la asignación de la responsabilidad para todos los eventos importantes a una persona en particular. En la segunda, debe permitir al

administrador responsable estar atento ante cualquier cambio en el esperado uso del sistema, con la finalidad de tomar la acción correctiva de forma adecuada y oportuna.

Ambas pruebas se limitan una a la otra. La prueba de contabilidad indica la grabación de una gran cantidad de datos, pero la grabación de demasiados datos puede dificultar la visibilidad.

Si un programa a ser auditable tiene un número significativo de instrucciones, se debe dividir en subprogramas, compuesto de módulos y de líneas de mayor nivel de código fuente, el cual generará instrucciones en lenguaje de máquina. Las comunicaciones entre estos subprogramas y módulos deberán ser claramente especificadas, debiendo registrarse el pase de información desde una persona que controla, a otra.

Cada programa debe conformar una especificación funcional que relaciona el medio ambiente entre sí (archivos, usuarios, otros programas, etc.). Las etiquetas, referencias y comentarios usados en el programa deberán ser claras y significativas. Así mismo, los listados deberán ser leíbles y significativos a otros.

Procedimiento de auditoría y control

- Rastrear una transacción por cada etapa del proceso y poder examinar los valores de datos intermedios que se producen en el procesamiento de la información.

- Imprimir registros y transacciones seleccionados del sistema que cumplan ciertos criterios, con la finalidad de validar la autenticidad y precisión de la información.

- Mantener un balance constante en el sistema, cuando se investigue la exactitud financiera de los registros y reportar si el sistema está balanceado.

- Emitir un diario detallado de las transacciones y los resultados de las mismas.

- Proporcionar los controles de entrada, es decir, verificar si son totales de control por documento y/o totales por paquetes o lotes, si existe la seguridad adecuada que garantice que sólo el personal autorizado entre a los datos del sistema, o si existe alguna manera de identificar al responsable de los datos de entrada.

En resumen un auditor necesita saber que: La entrada es correcta, completa y con registros de responsables, el procesamiento de los datos es correcto y con pistas de auditoría y la salida es correcta. y verificable.

CAPÍTULO 3

3. Principios y políticas de seguridad

3.1 Principios de seguridad

Se declara bajo “seguridad de informática” que la información y los sistemas deberán ser protegidos aplicando los siguientes principios:

3.1.1 Clara asignación de responsabilidades

La administración y mantenimiento de responsabilidades para los sistemas de computación y aplicaciones serán claramente definidas a través de la asignación de una persona directamente, por ejemplo: Administrador de base de datos.

3.1.2 Protección constante

Todos los equipos y sistemas de Computación (incluyendo los datos), deberán ser constantemente protegidos contra accesos no autorizados, cambios no autorizados, así como contra la destrucción deliberada de los mismos.

3.1.3 Autorizaciones objetivas

Permisos para la utilización de computadoras, redes de trabajo y sistemas de información, serán dados únicamente a las personas que necesitan tener acceso para el desarrollo de su trabajo dentro de la empresa.

3.1.4 Identificación efectiva de usuarios

Usuarios deberán ser plenamente identificables durante el uso de los sistemas de computación. Cada usuario es responsable por la correcta ejecución de sus tareas y con su propia identificación.

3.1.5 Monitoreo de las operaciones

Las operaciones en los sistemas de información deberán ser constantemente monitoreadas para cuestionar situaciones extrañas dentro de los mismos.

3.1.6 Recuperación después de una emergencia

Después de una interrupción no planificada (ejemplo: un desastre mayor, como inundación), el reinicio de actividades, deberá ser de acuerdo a los procedimientos de recuperación, respetando el período previsto de tiempo.

3.2 Políticas de seguridad

Todos los recursos de informática (equipo, programas y datos) deberán ser asignados a una persona responsable. La responsabilidad de informática es compartida con la persona responsable del recurso y la planeación, implementación, monitoreo y control de la seguridad, podrá ser delegada tomando en cuenta al responsable. Las políticas de seguridad son controles y procedimientos obligatorios para todos los sistemas de la organización, para asegurar la buena práctica de seguridad. Los controles de seguridad que van más allá de los procedimientos y estándares establecidos, deberán ser

justificados por el usuario, de acuerdo a sus necesidades de seguridad y su responsabilidad.

CAPÍTULO 4

4. Estándares de seguridad

4.1 Definición

La meta de la creación de estándares de seguridad, es proveer un juego de normas de seguridad para garantizar un nivel básico de confidencialidad, integridad y disponibilidad de los sistemas de computación dentro de la organización.

Estos estándares de seguridad deberán ser aplicados a todos los sistemas de computación, es decir: sistemas de información, redes de trabajo, computadoras personales y computadoras de escritorio.

A través de estas normas de seguridad, cualquier auditoría interna o externa se puede llevar a cabo de una manera eficiente, ya que la implementación de las mismas, permiten dejar huellas de auditoría.

Para un manejo más eficiente de seguridad, a cada recurso de informática se le asignará un "Propietario", es decir, una persona responsable del mismo. Esta persona podrá delegar responsabilidades sobre otras personas. Las siguientes funciones son establecidas como estándar:

- Propietario de la infraestructura de informática - Gerente de informática
- Propietarios de la aplicación y los datos - Usuarios finales

- Responsable por las operaciones en el sistema – Gerente de cada unidad de la organización.

- Responsable de la seguridad de informática – Gerente de informática.

El costo/efectividad de la seguridad, está basado en el manejo adecuado de los riesgos involucrados. Los propietarios de los recursos, son los responsables para la evaluación del costo/beneficio en la implementación de la misma.

Finalmente, las desviaciones en los estándares establecidos, deberán ser acordadas y documentadas por los responsables correspondientes (Gerente de informática y el usuario final). De cualquier forma, los controles obligatorios deberán ser implantados.

4.2 Controles obligatorios

Estos son controles mandatarios requeridos para la implementación de seguridad en informática. Estos controles aplican a todos los sitios de informática dentro de una organización.

4.2.1 Definición de los propietarios de los recursos

Todo recurso de informática (Equipos, programas y datos), deberá ser cuidados y controlados por una persona responsable. Esta persona podrá decidir sobre el nivel de seguridad para el recurso.

4.2.2 Definir controles de acceso

Todo los sistemas, aplicaciones y datos, deberán ser protegidos contra accesos no autorizados.

Computadoras y redes de trabajo de ambiente multiusuario que son utilizados por muchas personas deberán ser equipadas con una identificación de usuario y contraseña correspondientemente, que permita la restricción o autorización para el uso del mismo.

En casos especiales concernientes a la seguridad de los datos, medidas de protección adicional serán consideradas. Ejemplo: restricción de accesos (Tiempo, terminal específica), encriptación de bases de datos y/o archivos de usuarios, así como procedimientos que permitan una segura identificación del usuario.

4.2.3 Control de virus electrónicos

Todas las computadoras deberán ser protegidas contra virus electrónicos, a través del uso de programas que buscan virus. En computadoras personales y terminales de trabajo, el programa de Anti-virus, deberá estar activo constantemente trabajando en Background. Sí esto no es posible, entonces revisión de virus, será ejecutado diariamente a través de una función automática durante el arranque del equipo. El software de Anti-virus deberá ser actualizado constantemente para la búsqueda de nuevos tipos de virus.

4.2.4 Derechos de autor

Por razones legales de “derechos de autor”, los programas de computadora no podrán ser copiados o pasados ni aceptados, sin la licencia correspondiente.

4.2.5 Regulaciones con consultores

Cuando sea necesario trabajar con consultores, se deberán definir regulaciones de seguridad y reglas específicas para ser seguidas.

4.2.6 Educación a usuarios

Los usuarios deberán ser educados y hacerles conciencia de su responsabilidad en el manejo de los datos y los procedimientos de seguridad a cumplir.

4.2.7 Control de incidentes de seguridad

Los empleados deberán reportar los incidentes de seguridad que se susciten durante la rutina de trabajo al propietario del recurso afectado.

4.2.8 Plan de recuperación en caso de desastre

La organización será protegida contra desastres mayores por una implementación de procedimientos de recuperación, en lo que se refiere a computadoras y datos.

4.2.9 Regulaciones legales

El diseño, operación y uso de recursos de informática, deberán cumplir con las regulaciones legales establecidas por la organización y por el estado.

4.3 Control de recursos de informática

Como se mencionó, todo recurso deberá ser cuidado y contabilizado a fin de asociarle un propietario, a quien se le asignará dicha responsabilidad, como se describe a continuación:

4.3.1 Responsabilidades

Ser propietario del recurso significa tener un cuidado personal del mismo, como si en realidad fuera el dueño. Su responsabilidad está referida por la seguridad y mantenimiento del recurso de informática.

4.3.2 Recursos a ser asignados

- Recursos de datos: archivos de datos, bases de datos, documentación, reportes impresos.
- Recursos de Software: Sistemas de Información y aplicaciones de computadoras
- Recursos de Hardware: Computadoras y equipo de comunicación
- Recursos de respaldos: Cartuchos, Discos
- Recursos de servicios: Programas fuentes
- Otros: fuentes de poder (UPS), equipo de aire acondicionado, mobiliario, etc.

4.3.3 Protección de recursos de informática

Computadoras, redes de trabajo, programas y datos deberán ser protegidos contra mal uso, cambio, robo y destrucción.

4.3.4 Protección de instalaciones

Localidades para los servicios de informática y/o equipos, deberán ser construidas, arregladas y equipadas para proveer protección contra daños provenientes por sabotajes y

desastres naturales como fuego, terremotos, así como robos y acceso no autorizados. Las áreas que contengan equipo crítico para la organización serán protegidas por construcciones específicas, custodiadas por guardias de seguridad, puertas de acceso electrónico, cámaras de circuito cerrados, etc.

Por supuesto, toda medida de seguridad deberá ser consistente con el riesgo concreto y con el recurso y/o servicio resguardado.

4.3.5 Protección de sistemas y datos

Adquisición de equipo

Todo recurso de informática que se adquiera deberá permitir la implementación de las medidas de seguridad estándares de la organización.

Ingreso de datos

El ingreso de datos para ambientes productivos deberá ser ejecutados por personas autorizadas. Este ingreso deberá ser revisado para correcciones lo que dependerá del nivel de importancia de los datos. Estas revisiones pueden ser por medio de chequeo visual, reingreso de datos para verificación, verificación aritmética y cualquier otro método o sistema que permita la validación de datos.

Rastreo / Huellas de auditoría

Los recursos para el ingreso de datos en ambientes productivos, deberán dejar rastro para propósitos de validación (Cuándo, Cómo, Quién ingresó los datos).

Transmisión de datos

Para toda aplicación empleada para la transmisión de datos, texto, voz o imágenes, el propietario del recurso, deberá determinar cuando será necesario encriptar o asignar una contraseña.

Para accesos desde redes públicas, adicionales elementos de seguridad deberán ser utilizados, además del uso obligatorio de identificación de usuario y contraseña. Por ejemplo: Tarjetas de identificación de usuarios, software avanzado para la autenticación de usuarios, servicios de CallBack y otros.

Integridad de sistemas

Se deberán utilizar aplicaciones que permitan la validación y verificación de accesos no autorizados con el propósito de evitar alteración a los datos. Estas aplicaciones deberán: validar usuarios, claves y niveles de seguridad.

Redundancia de equipos

Averías a equipos críticos para la organización pueden causar largas interrupciones de trabajo. Estas podrán ser prevenidas a través de trabajar con unidades de redundancia, tales como servidores en línea, discos en espejo, tener repuestos en bodega, etc.

4.4 Protección de equipos de usuarios

4.4.1 Robo y destrucción

Recursos de informática instaladas en área de usuarios (computadoras personales, Terminales, Impresoras, etc.), deberán ser aseguradas para prevenir el robo y destrucción.

Los medios más comunes para dicha protección son: Guardias de seguridad, Puertas con accesos electrónicos, cámaras de circuito cerrado, etc.

Para el almacenamiento de datos a través de Cartuchos, Disquetes, discos compactos, se deberán utilizar cajas porta disquetes / discos compactos. En el caso de cartuchos que son utilizados como parte del plan de recuperación, los mismos se deberán almacenar en un lugar distinto en donde se encuentra los datos.

4.4.2 Seguridad en computadoras portátiles

Hay dos aspectos particularmente importantes en los equipos portátiles de computación:

- Primero, su valor y pequeñas dimensiones que son un blanco fácil para los ladrones.
- Segundo, computadoras portátiles no sólo son usadas en laboratorios u oficinas, sino también en varios ambientes que son menos seguros.

En adición, en caso de pérdida del contenido del equipo(la valiosa información) usualmente agrega serios daños que el valor mismo de la computadora portátil y la recuperación toma tiempo y pérdidas hasta que los datos y programas han sido recuperados, si es posible recuperar todo. El peor daño ocurre cuando la información cae en las manos equivocadas esto puede ser por el ladrón o por negligencia del dueño de la computadora.

El valor de la computadora portátil, los programas y los datos requiere que la computadora sea usada y mantenida con cuidado y responsabilidad, por lo que las

regulaciones deben ser estrictamente observadas ejemplo: Derechos de copia, derechos de autor y confidencialidad.

Programas y datos aprobados

Los programas, aplicaciones y datos usados fuera de la organización deben de ser explícitamente aprobados por el responsable de la aplicación y dueño de los datos.

Usuarios autorizados únicamente

El dueño es el responsable de que el equipo portátil no sea usado sin una formal autorización.

4.4.3 Manteniendo el equipo en buen estado

Mantenimiento y cuidado

El equipo portátil debe estar mantenido por el dueño en buenas condiciones de trabajo. El equipo debe ser limpiado y no se debe exponer a daños intencionales como calor, exceso de frío, humedad vibraciones, fuertes, campos magnéticos y otros daños que se pueden prevenir.

Fuente de poder

Para mantener la funcionalidad del equipo, el sistema de poder debe estar bien mantenido, las baterías deben ser cargadas en tiempo, seleccionar adecuadamente el voltaje. Las computadoras portátiles siempre se deben apagar cuando no están en uso.

4.4.4 Protección de datos y programas

Prevenir ingresos sin autorización

Las computadoras portátiles deben ser protegidas por una contraseña de arranque. Esta característica previene el encendido sin autorización del disco duro o de un disquete. Si un mecanismo físico de seguridad es disponible es recomendado utilizarlo para no habilitar el uso del equipo.

La computadora no debe ser dejada sola cuando esta en estado operacional. Para prevenir ilegítimas manipulaciones, se debe programar el equipo para que se desconecte después de 5 minutos de no estar en uso y que sea necesario una contraseña para reactivar el estado operacional del equipo Ejemplo: En algunos modelos para el ahorro de energía el equipo se coloca en *estado inactivo* y automáticamente se puede asegurar el equipo para ingresos no autorizados.

Encriptado protección especial de la información

Para asegurar la confidencialidad y los datos críticos que se encuentran en el disco duro de una computadora portátil, estos deben ser encriptados. En cooperación con el responsable del dueño de la información se debe determinar que clase de encriptado se utilizará. También debe ser discutida y tener una copia de respaldo cuando la información es transmitida vía una red.

Una de las funciones muy importantes de los responsables de comunicaciones es mantener controlado el uso de los datos de la compañía y los sistemas de transmisión.

Además de controlar el uso del sistema por empleados autorizados, deben también considerarse los problemas relativos a empleados que pueden tener acceso al computador, pero que no están autorizados a usar programas o acceder a los ficheros de bases de datos, así como los problemas con individuos ajenos a la organización.

Un sistema de información puede ser causa de violación de su seguridad, debido a varios factores:

- La naturaleza de la organización y de sus operaciones.
- Los tipos de aplicaciones y de bases de datos en el sistema de proceso de datos.
- La posibilidad de beneficio económico para los delincuentes.
- El tamaño de la población de usuarios del sistema.
- El tipo de sistema y las posibilidades disponibles para los usuarios.
- Las amenazas potenciales contra un sistema de proceso de datos y las pérdidas que pueden producirse, son razones suficientes para la estimación de riesgos contra la seguridad.

La protección de información reservada en un canal de comunicación, es esencial. Uno de los principales métodos para ofrecer protección es hacer que la información del mensaje sea ininteligible por medio de técnicas criptográficas, sin intentar ocultar la existencia del mensaje.

Encriptación

Es una técnica mediante la cual se transforman los datos de forma que no proporcionen información al ser interceptados, puesto que tal como están almacenados o transmitidos son completamente ininteligibles.

Cada carácter es un registro reemplazado por otro carácter, así por ejemplo:

La palabra SMITH se almacena como @LAZ#

En este caso, toda S es reemplazada por el símbolo @, etc., de este modo si alguien obtiene los datos no los entenderá, a menos que el lector sepa cómo descifrar la información.

La mayor aplicación de escribir los datos usando criptografía, se aprecia en la protección de los mismos cuando se transmiten a través de las líneas de comunicación.

Elementos de la criptografía

Los mensajes que deben ponerse en clave se conocen como texto en claro y, a la operación en que los símbolos básicos se transponen o sustituyen para transformar los datos, se denomina puesta en cifra. La salida de procesos de puesta en clave se conoce como texto cifrado o *criptograma*, que luego es transmitido.

La persona que intenta accesar a la información puede escuchar y copiar cuidadosamente el texto cifrado completo. Sin embargo, a diferencia del receptor asignado, dicha persona no conoce la clave y por lo tanto, no puede descifrar con facilidad dicho texto. En algunas ocasiones el intruso no sólo escucha la comunicación que se hace a través del

canal (intruso pasivo), si no también puede registrar los mensajes y repetirlos posteriormente, incluir sus propios mensajes, o bien, modificar los mensajes originales antes de que lleguen al receptor.

El hecho de quebrar el cifrado se conoce como criptoanálisis y, el de inventar cifras, criptografía y desbaratarlas, como criptología.

Propiedades de las técnicas de cifrado

Las técnicas de cifrado deben tener las siguientes propiedades:

- Para los usuarios autorizados debe ser relativamente sencillo cifrar y descifrar datos.
- El esquema de cifrado no depende de mantener en secreto el algoritmo, sino de un parámetro del algoritmo llamado clave de cifrado. Para un intruso debe ser muy difícil determinar cuál es la clave de cifrado.

Método de cifrado

Los métodos de cifrado se dividen en dos categorías: cifradores de substitución (incluyendo los códigos) y cifradores de transposición.

Cifradores de substitución

En un cifrador de substitución, cada letra o grupo de letras se substituyen por otra letra o grupo de letras de un alfabeto cifrado.

El cifrado más antiguo es el Cifrado de César. En este método a se representa por D, b por E, c por F, y z por C. Por ejemplo: ataquen se representa por dwdtxhq.

Una generalización sencilla de este método permite que el alfabeto cifrado se desplace k letras, en lugar de 3. En este caso, k se convierte en una clave para el método general de alfabetos desplazados en forma circular.

Una mejora de este método consiste en correlacionar cada uno de los símbolos del texto en claro con alguna otra letra, por ejemplo:

Texto en claro: abcdefghijklmnopqrstuvwxyz

Texto cifrado: QWERTYUIOPASDFGHJKLZXCVBNM

Substitución monoalfabética

A este sistema se le conoce como *substitución monoalfabética*, en la cual la clave se constituye por una cadena de 26 letras, correspondiente al alfabeto completo. Así: ataquen sería QZQJXTF.

Aparentemente, este sistema puede ser seguro por que aún, cuando el criptoanalista conociera el sistema general (substitución letra por letra), no conoce cual de las 26. =4x4026 posibles claves está empleándose. No es factible probar todas las claves como en el cifrado de Cesar. Sin embargo, el cifrador puede desbaratarse fácilmente mediante las propiedades estadísticas de los lenguajes naturales, es decir, por la frecuencia con que una letra se presenta en un idioma dado.

Cuando un criptoanalista intenta desbaratar un cifrado monoalfabético comienza contando las frecuencias relativas de todas las letras que aparecen en el texto cifrado. Después le asigna en forma tentativa una letra, luego del cual supone otra letra para

aquella que le sigue a la de mayor frecuencia. Por medio de suposiciones con las letras, el criptoanalista genera un texto tentativo, letra por letra.

Cifrado polialfabético

Es el resultado de introducir múltiples alfabetos de cifrado que se utilizan en rotación, cuyo objetivo es adecuar las frecuencias del texto cifrado, de forma tal que las letras con mayor frecuencia de aparición no sobresalgan tan claramente.

Dentro de este sistema se tiene el cifrado vigenere, que consiste de una matriz cuadrada que contiene 26 alfabetos de César.

El primer renglón llamado renglón A es ABCDEFGH....XYZ.

El siguiente renglón, llamado renglón B es BCDEFGHI....YZA

Finalmente: El último renglón llamado renglón Z es ZABCDEFG....WXY.

De forma similar al cifrado monoalfabético, este cifrado también tiene una clave, pero ya no es una cadena de 26 caracteres diferentes sino una palabra o frase corta y fácil de recordar.

Cuando se pone en clave un mensaje, la clave se escribe en forma repetida en la parte superior del texto en claro. Así: CLAVECLAVECLAVECLAVECLAVECL

gerenteviajalunesenlamañana

La letra clave que se encuentra sobre el texto en claro indica el renglón que se debe utilizar para la puesta en clave. La g se pone en clave usando el alfabeto de Cesar del

renglón C, la e y la r, los renglones L y A. Una letra de texto se representa mediante diferentes letras en el texto cifrado, dependiendo de la posición en el texto claro.

Un cifrado polialfabético puede ser muy eficaz si se usan cifrados monoalfabéticos arbitrarios para los renglones, en lugar de restringirlos al cifrado de Cesar, aunque tiene el inconveniente de que la matriz de 26x26 también se convierte en parte de la clave y se deberá memorizar o escribir.

Un criptoanalista puede desbaratar el cifrado dando una longitud supuesta de la clave. Si la longitud de la clave es K, ordena el texto cifrado en renglones tomando K letras por renglón. Si su suposición es correcta, todas las letras del texto cifrado en cada columna se ponen en clave mediante el mismo cifrador monoalfabético, en caso contrario se prueba con otro valor.

Otra de las formas de dar mejor complejidad al cifrado es utilizar una clave que sea de mayor longitud que la del texto en claro. Para ello se escoge como clave una cadena de bits aleatoria. Después, se convierte el texto en claro en una cadena de bits (puede ser su representación en ASCII). Por último, se aplica un OR EXCLUSIVO, bit por bit, con estas 2 cadenas. De este modo, el texto cifrado no puede desbaratarse puesto que todos los posibles textos en claro son candidatos, igualmente probables y no le proporcionará ninguna información al criptoanalista.

Las desventajas que tiene este método, conocido como clave de una sola vez, son las siguientes:

La clave no se puede memorizar por lo cual debe escribirse.

La cantidad total de datos que puede transmitirse se limita por la cantidad de clave disponible.

La sensibilidad del método ante la pérdida de mensajes.

Cifradores de transposición

A diferencia de los cifradores de substitución, que reemplaza las letras del texto en claro por símbolos, los cifradores de transposición reordenan las letras. La clave del cifrador es una palabra o frase que no contiene una letra repetida. La finalidad de la clave es la numeración de las columnas, siendo la columna 1 la que queda bajo la letra de la clave más cerca al inicio del alfabeto y así sucesivamente.

El texto en claro se escribe horizontalmente en renglones y el texto cifrado, se lee por columnas comenzando en la columna cuya letra clave tiene el valor inferior.

Para desbaratar el cifrado, el criptoanalista debe reconocer primero el tipo de cifrado (substitución o transposición). En este caso se debe observar la frecuencia de las letras de aparición más común y si se adaptan al patrón normal del texto en claro.

Luego supone el número de columnas o longitud de la clave para ordenarlas.

Cuando el número de columnas K es pequeño, cada uno de las K(K-1) pares de columnas se pueden examinar para ver las frecuencias de las letras. El par de mayor correspondencia es el que está colocado en la posición correcta y se prueban después las columnas restantes para ver cuál le sigue a ese par. El proceso continúa hasta que se encuentra un orden probable.

Norma de cifrado de datos

La Norma de Cifrado de Datos (Data Encryption Standard: DES) es un algoritmo de cifrado desarrollado por la IBM , que fue aprobado por la Oficina Nacional de Normas de los Estados Unidos en 1977, como una Norma Oficial para información no clasificada y para ser usada por los sistemas de comunicaciones de los sectores privado y gubernamental.

Esta norma (DES), es una transformación producto, es decir, que utiliza los conceptos de transposición y substitución, cuyo objetivo es el de hacer un algoritmo de cifrado tan complicado, de modo que un criptoanalista no tenga ninguna posibilidad de obtener información de un texto cifrado.

Cifradores producto

Es un circuito empleado para las transposiciones y substituciones se realiza así:

1)Una caja P (permutación) para una transposición de 8 bits, que se efectúa mediante un cableado interno.

2) una Caja S que se utiliza para la substitución. Se tiene como entrada un texto en claro de 3 bits, que selecciona una de las 8 líneas que salen de la primera etapa y la fija con un valor 1 y todas las demás 0. La segunda etapa es una caja P y en la tercera se codifica la línea de entrada seleccionada.

3) un Cifrador Producto, combinación de las 2 anteriores. En la primera etapa se transpone 12 líneas de entrada que se dividen en cuatro grupos de 3 bits, cada uno de los cuales se substituye en forma independiente a las demás.

Algoritmo DES (Data Encryption Standard)

La transformación DES es una cifra-producto de bloques no lineal, iterativa, que opera sobre bloques de datos de 64 bits. Es muy compleja y es apropiada únicamente para ser operada por medio de computadoras.

El algoritmo DES se utiliza en forma inversa para descifrar el texto cifrado (utilizando la misma clave).

El cifrado del texto en claro se realiza en bloques de 64 bits que produce 64 bits de texto cifrado. Se parametriza por una clave de 56 bits.

La primera etapa es una transposición independiente de la clave sobre el texto en claro de 64 bits. La última etapa es exactamente la inversa de esta transposición. La penúltima etapa intercambia los 32 bits de la parte izquierda con los 32 bits de la derecha. Las 16 etapas restantes son funcionalmente idénticas, pero tienen diferentes funciones de la clave.

La función consta de 4 pasos secuenciales:

1. Se construye un número E de 48 bits mediante la expansión de los 32 bits Ri-1,de acuerdo con una regla fija de transposición y duplicación.

2. E y Ki, se someten conjuntamente a una función OR EXCLUSIVO.

3. La salida se divide en 8 grupos de 6 bits, cada uno de los cuales alimenta a una caja-S diferente, que producen salidas de 4, en lugar de 6 bits. Cada una de las 64 posibles entradas a una caja-S se corresponde con salidas de 4 bits.

4. Los 32 bits se pasan por caja-P

En cada una de las 16 iteraciones se utiliza una clave diferente. Antes de que comience el algoritmo, se aplica una transposición de 56 bits a la clave. Antes de cada iteración se divide la clave en dos unidades de 28 bits, las cuales se rota a la izquierda según número de bits que depende del número de iteración.

El valor de Ki se deriva de esta clave rotada por medio de la aplicación de otra transposición de 56 bits sobre ella.

Existen 2 maneras de fortalecer la norma DES:

1. Incluir caracteres aleatorios en el texto en claro, por medio de una regla definida. Por ejemplo, todos los n-ésimos caracteres son reales y el resto son sólo ruido.

Además, se pueden insertar mensajes de relleno entre los que son reales. Este principio se conoce como *Cifrador Nulo*, por el cual se tiene un desperdicio de ancho de banda pero cuyo descifrado es muy difícil porque la posición de los caracteres reales y de los mensajes se conserva en secreto y se cambia cuando se modifica la clave.

2. Otra manera más difícil, es hacerla funcionar como un *Cifrador de Flujo*, en el que tanto el transmisor como el receptor operan sus circuitos integrados DES en modo de cifrado (opuesto al descifrado).

Aplicaciones de la criptografía

La aplicación de un tipo de transformaciones de cifrado en un sistema de teleproceso o de archivo, depende de las características de una aplicación en particular y de los aspectos técnicos del sistema. Aunque la finalidad del cifrado es dar seguridad a los datos almacenados o en tránsito, sus efectos sobre utilidad de una aplicación también son importantes.

Las características de una aplicación que determinan la elección del método de cifrado son:

- El valor de la información a proteger.
- El tipo de lenguaje utilizado (lenguaje natural o de programación).
- Dimensiones y dinámica de la aplicación (volumen de mensajes o registros que deben transmitirse o almacenarse, las velocidades y tiempos de respuesta exigidos).
- Características de las transformaciones criptográficas
- El tamaño de la clave debe ser muy grande para dificultar los intentos de descubrirla.

Las características del lenguaje (frecuencia de letras, pares de letras, etc.) deben quedar enmascaradas y alteradas. La transformación debe ser muy compleja para evitar el análisis matemático. Las transformaciones, por ejemplo, la substitución poligráfica de un carácter por un grupo de caracteres, aumentan la longitud del mensaje cifrado sobre la del original.

En las situaciones simples no hay propagación de errores, ya que se aplican sobre cada carácter independientemente, a diferencia de los cifrados por bloques que se propagan a lo largo del bloque o texto cifrado subsiguiente.

La longitud de la clave es importante para dificultar el criptoanálisis. Las claves cortas del mensaje deben aplicarse repetidas veces en el proceso del cifrado. Las claves más largas que el mensaje, elegidas aleatoriamente y que se utilizan sólo una vez, son más seguras. De acuerdo al tipo de transformación, estos sólo pueden funcionar cuando los dispositivos de cifrado/descifrado están sincronizados en el tiempo, por cuya pérdida se puede impedir el descifrado correcto.

4.4.5 Anticipar un robo

Para prevenir la pérdida de un equipo a través de un robo, la computadora siempre debe estar guardada en un lugar seguro. Cuando se viaja durante el equipo no se debe dejar sin atender tener en mente que es un equipo pequeño y que es fácil de robar.

Si el robo de todas formas se ejecuta, se debe minimizar el daño, la seguridad debe ser una meta:

- No tener daños en la confidencialidad
- No perder ningún dato que no pueda ser recuperado
- Re escribir y recuperar todos los datos que sean posibles
- El daño debe ser limitado

Las siguientes precauciones ayudaran a mantener el daño limitado si la computadora portátil es robada:

- Información confidencial que no es requerida para ejecutar un trabajo no debe ser llevada en el disco duro.

- Información confidencial no debe ser legible por un lector que no esta autorizado ejemplo encriptar la información.

- Nuevos datos y nuevos procesos deben ser copiados a una copia de respaldo todo el tiempo.

- Copias de respaldo críticas no deben ser llevadas en el mismo lugar donde se encuentre la computadora portátil.

- Si la computadora es robada o perdida todas las personas involucradas en los datos, aplicaciones e información deben de ser informadas inmediatamente.

Procedimientos de seguridad

Cuando se este utilizando las computadoras portátiles todas las regulaciones relevantes a la seguridad deben ser estrictamente observadas. Durante el trabajo con el equipo el usuario debe ejecutar las funciones de seguridad planeadas ejemplo: Protección del equipo y datos frecuentes, creando copias de respaldo, seguir los procedimientos formales de transmisión de datos del equipo portátil a otros sistemas.

Las circunstancias de trabajo con una computadora portátil (hoteles, trenes, aviones etc.) son normalmente menos seguras que en un ambiente bien controlado de oficina, por lo

tanto todos los datos enviados desde una computadora portátil a otros sistemas deben ser verificados por programas antivirus.

4.4.6 Funcionalidad

Para cada recurso de informática, una persona será asignada como responsable (para computadoras personales usualmente es el usuario). Esta persona se deberá asegurar a través de mantenimientos y supervisión, sobre la correcta funcionalidad del mismo, así como la utilización únicamente por personas autorizadas.

4.4.7 Archivos de usuarios

A través de la utilización de procedimientos de respaldo, los archivos y aplicaciones de usuarios serán asegurados en el caso de algún problema al equipo correspondiente.

También, estos serán protegidos contra acceso no autorizados, mediante el uso de Contraseña, bloqueo automático de la aplicación (contraseña de protectores de pantalla) o del equipo.

Determinación de contraseña personal

Cada usuario debe de asignársele una contraseña personal. Hoy en día los sistemas proveen sofisticados métodos de almacenamiento de contraseñas los cuales no pueden ser accesados ni por los especialistas, y quedan para ser cambiadas únicamente por los usuarios que conocen la contraseña vigente.

Contraseñas para varios ambientes

Todas las contraseñas de todos los ambientes son igualmente importantes, pero hay diferencia entre un sistema y otro en el manejo de las contraseñas, por lo que se recomienda que se exploten las fortalezas de cada uno de estos y se tomen las precauciones debidas para las debilidades que cada uno tenga.

Confidencialidad en correos electrónicos

Para enviar correos electrónicos, se deben de tomar ciertos cuidados de confidencialidad para garantizar la seguridad de los documentos que se envían, lo más apropiado es hacer una copia del documento de elaborado en procesador de palabra que se va enviar protegiéndolo con contraseña, luego adjuntarlo al correo electrónico, y posteriormente en otro correo electrónico ya sea antes o después enviar la contraseña para que pueda ser abierto, o bien tener una metodología de contraseñas para que el receptor puede descifrarla, por ejemplo:

Caracteres	1 y 2	iniciales de la persona que envía
	3 y 4	número del día en que se envía
	5 y 6	iniciales del receptor

Existen herramientas las cuales sirven para proteger la información a varios niveles como sistemas operativos, correos electrónicos, poderosos algoritmos de encriptación las cuales son rutinas que deben de ser transparentes para el usuario final, para lo cual se recomienda tener una completa herramienta en la computadora personal que permita la

encriptación y autenticación de correos electrónicos, archivos y discos. Se recomienda instalar herramientas en el servidor para autenticación de usuarios y contraseñas que puedan encriptar correos electrónicos y archivos, se puede determinar el manejo de estos con llaves que pueden ser de carácter público y garantizar confidencialidad con llaves privadas.

Contraseña de usuario

Las computadoras personales y cualquier otro tipo de computadoras, de todas formas serán protegidas por la contraseña de usuario en el sistema correspondiente o una medida de seguridad equivalente, sí la misma está conectada a una red de trabajo o si tiene almacenada información sensitiva, en tal caso el drive de disquete será protegido.

Mantenimiento de medios de almacenamiento de datos

Todo medio de almacenamiento de datos con información confidencial que necesite ser reparado, la misma deberá ser efectuada únicamente bajo la supervisión del propietario correspondiente. También, los medios de almacenamiento de datos que en el futuro ya no serán utilizados, se deberán destruir.

Protección en ambientes externos a la organización

Colaboración en informática con otras organizaciones o instituciones significa:

- Consultores externos trabajando con los sistemas de la organización
- Procesa miento de datos en otras computadoras

Cuando se está trabajando con consultores, todos los reglamentos estándares de seguridad son validos. Adicionalmente, deberán seguirse las siguientes normas:

Un empleado específico será responsable en el trabajo conjunto con el consultor. Dentro del contrato con el Consultor, se deberá regular que el consultor manejará la información con estricta confidencialidad. La información que será utilizada por el consultor, deberá contar con la explícita autorización del propietario de la misma.

4.5 Administración de usuarios y estándares de seguridad

Permiso para el uso de los sistemas será dado únicamente a las personas que necesitan desarrollar su trabajo dentro de la organización.

La autorización del uso del los sistemas y su comunicación puede ser gobernados por propiedades estándares y características físicas estándares de la comunicación. Las propiedades de las aplicaciones especificas han sido debatidas por muchas organizaciones y han propuesto sus propios estándares:

The International Standard Organization (ISO)

Es la organización que facilitó la creación voluntaria de los estándares. ISO 7816 es la parte del documento de estandarización concerniente a seguridad de las comunicaciones electrónicas.

National Institute of Standards and Technology (NIST)

Publica un documento conocido como FIPS 140 "Requerimientos de seguridad". Este documento trata sobre los requerimientos físicos, electrónicos y lógicos de seguridad y su comunicación.

EUROPAY, MasterCard and Visa

Han creado su documento " Especificaciones para tarjetas de circuitos integrados para sistemas de pagos". La especificación intenta crear técnicas comunes básicas para sistemas de tarjetas en su implementación y almacenamiento de datos.

Microsoft

Ha propuesto documentos para la implementación de seguridad en medios electrónicos ejemplo PC/SC que aplica únicamente a la CPU cards.

Comité Europe Normalisation (CEN) and European Telecomunications Standards Institute (ETSI).

Este instituto tiene como principal objetivo normar las telecomunicaciones así como el GSM SIM para teléfonos celulares. GSM 11.11 and ETS1300045.

4.5.1 Permisos para operación y uso

Todo recurso de informática será operado por personas quienes cuentan con la autorización del responsable correspondiente.

4.5.2 Autorización de usuarios

Toda autorización para el uso de los recursos de informática será emitida por el responsable de área y/o por el propietario del mismo. Tanto la identificación del usuario como la contraseña será asignada por éste último.

Los usuarios podrán ejecutar únicamente aquellas actividades a las cuales se les ha dado autorización previamente.

4.5.3 Registro de usuarios

El uso de cualquier recurso de informática deberá tener un documento formal de registro. Este documento deberá ir firmado por el usuario, el responsable del área y el propietario del recurso.

A los usuarios se le deberá indicar sobre la confidencialidad de los datos que manejará así como los niveles de autorización y privilegios que se les ha asignado.

La identificación deberá ser única y no se podrá transferir a otra persona y cuando el empleado se retire de la organización , su identificación deberá ser eliminada del sistema para futuras auditorías.

El responsable del área deberá tener el cuidado de actualizar cualquier cambio al perfil de cada usuario (nivel de seguridad, privilegios, etc.)

4.5.4 Autorizaciones especiales

Ciertos privilegios que son requeridos por especialistas, para determinadas funciones de informática, serán emitidas por el responsable del área y el propietario del recurso. Estas

autorizaciones deberán ser para tareas claramente definidas y para un límite reducido de personas. Ejemplo de especialistas: Auditores.

4.5.5 Autorización de grupos

Cada usuario será normalmente identificado de forma individual, sin embargo, algunas veces se requiere de autorizaciones de grupo donde todos los usuarios que pertenecen a un mismo grupo, se identifican por un mismo usuario y una misma clave. Por lo tanto, esta regla será manejada como una excepción y por razones bien fundamentadas. De cualquier forma, un usuario que pertenezca al grupo será el responsable por el manejo de la contraseña.

4.5.6 Identificación de usuarios

Cada usuario será confiablemente identificado durante el tiempo de operación dentro del sistema de informática. Este será el responsable por las tareas que está ejecutando con su identificación.

4.5.7 Autenticación

Cada persona que trabaja dentro del sistema, será identificada a través de algún método de autenticación como: Contraseña, PIN, Tarjeta electrónica, Autenticación dactilar.

Cuando se está trabajando con sistemas críticos para la organización o en ambientes vulnerables, medidas adicionales pueden ser tomadas como por ejemplo: Servicio de CallBack, doble contraseña, algún software especial de autenticación.

SMART CARD

Es una tarjeta plástica que tiene un microprocesador que almacena y permite transacciones entre usuarios. Esta información esta asociada con el valor de la información así como su almacenamiento y su procesamiento. Esta tarjeta es parte de un sistema de computación que utiliza un lector que le permite la comunicación con el resto del sistema y su uso se ha extendido a varias aplicaciones: bancos, cuidado de la salud, transporte, entretenimiento y seguridad.

Las Smart Card mejoran la seguridad de cualquier transacción identificando al usuario y su cuenta. También proveen componentes vitales de seguridad en el sistema a través del intercambio de información virtualmente en cualquier componente de la red de información. Tiene un gran rango de seguridad desde un almacenamiento descuidado del usuario hasta sistemas sofisticados de contraseñas.

Seguridad basada en un sistema Smart Card

Un sistema de seguridad basado en una tarjeta es típicamente una tarjeta con un microprocesador que es tratado con una parte activa del sistema de computación.

La interacción entre el usuario y la tarjeta puede ser una serie de pasos que determinan si la tarjeta es autorizada para ser usada en el sistema, el proceso identifica si el usuario puede ser identificado, autenticado y si la tarjeta presenta las credenciales apropiadas que conduzcan a la transacción. La tarjeta puede también demandar lo mismo del usuario antes de proceder con una transacción.

El acceso a una información específica en la tarjeta es controlada por: El sistema operativo interno de la tarjeta y los permisos preestablecidos de la tarjeta de acuerdo a las condiciones del archivo.

Hay varios pasos básicos a seguir para asegurar el sistema de Smart Card, de acuerdo al tipo o tamaño: Análisis: Tipo o tipos de seguridad los datos, usuarios, puntos de contacto, transmisión, relativos riegos/impacto de la pérdida de datos, despliegue del sistema por el propietario del sistema, localización de debilidades: Intentos y/ó ataques al sistema, aprender sobre los puntos débiles.

Cuando se analizan los datos y su organización se debe tener en cuenta muy de cerca dos áreas especificas: ataques internos y externos. El primero es el más común y viene usualmente de los empleados inconformes, conociendo esto un buen propietario de la información separa todas las copias de respaldo y el sistema de respaldo en forma separada y en un lugar seguro. La introducción de virus y el intento de borrar los discos del sistema es un ataque típico interno.

Utilizando smart cards para los empleados que trabajan en el sistema se pueden evitar los ataques internos porque se registra la hora de uso, fecha, archivos y equipos utilizados, así mismo la tarjeta smart card deshabilita este tipo de ataques.

Los ataques externos usualmente se ejecutan donde la seguridad del sistema es débil, interceptando la transmisión de datos. La utilización de smart card refuerza el sistema en su seguridad por las propiedades descritas.

Análisis de la seguridad requeridas en el sistema utilizando Smart Card

El siguiente grupo de preguntas es relevante en el análisis de la seguridad:

¿Es encriptada la transmisión de datos en la tarjeta?

¿Son transmitidos los datos o copiados del lector al usuario final encriptado?

¿Envía el usuario los datos encriptados?

¿Se establece protocolos de seguridad con diferentes llaves?

¿Tiene el sistema código de seguridad para cargar y descargar?

¿Se entiende el sistema legal referente a la seguridad y derechos de autor?

¿Tiene el fabricante de las tarjetas un lugar seguro para el almacenamiento de las mismas?

Estándar ISO 7816-1,2,3

Parte #1: Características físicas ISO 7816-1:1987

Define las dimensiones de contacto del las tarjetas y su resistencia a la electricidad estática, radiación electromagnética y resistencia mecánica. También define la localización física de la banda magnética y el área para firma.

Parte #2: Dimensiones y localización de contacto

ISO 7816-2:1988 define la localización características eléctricas de los contactos de la tarjeta.

Parte #3: Señales electrónicas y transmisión de protocolos

ISO 7816-3:1989 define requerimientos de corriente y voltaje para los contactos eléctricos definidos en la parte 2 y protocolo half duplex carácter transmisión protocol T=0, corrección 1:1992 protocolo tipo T=1 half duplex block transmisión protocol, Smart card transmisión protocol T=14.

Parte #4: Comandos inter-industria para intercambio ISO 7816-4

Establece un grupo de comandos para todas las industrias que proveen acceso, seguridad y transmisión de datos por tarjetas, comandos para leer, escribir y actualizar datos.

Parte #5: Sistema de numeración y procedimiento de identificación de aplicaciones ISO 7816-5: 1994

Establece estándares para identificación de aplicaciones.

Parte #6: Elementos de datos inter-industria ISO 7816-6

Detalla la transportación física del equipo, protocolos de transmisión. Las especificaciones permiten la transmisión de dos protocolos, Carácter protocol T=0 or block protocol T=1, una tarjeta puede soportar uno pero no los dos.

4.5.8 Manejo de contraseña

Toda contraseña deberá manejarse de forma confidencial y personal. El usuario correspondiente es el único responsable del mismo y a él se le permitirá definirlo personalmente a través un procedimiento determinado y periódicamente por el sistema de forma automática.

4.5.9 Regulación de contraseña

Las siguientes reglas se aplicaran para el uso de contraseña en computadoras:

- Por lo menos 5 posiciones para la longitud. Se debe crear con letras y números preferiblemente expresiones que no son fáciles de adivinar se deberán usar

- Cambio cada 60 días como mínimo. El usuario podrá cambiar la contraseña cada vez que lo desee. La misma contraseña podrá ser utilizada después de un año de haber transcurrido el cambio.

4.5.10 Contraseña inicial

Cuando se ha entregado la contraseña al usuario, la misma deberá ser cambiada y personalizada inmediatamente por el usuario.

Contraseñas estándares entregadas por el fabricante de algún recurso de informática, ya sea equipo o programa, se deberá cambiar por el propietario del recurso o por el responsable de área.

Las aplicaciones que permitan deberán ser configuradas para que después de 30 minutos de inactividad, la misma se desactive automáticamente.

También, después de 3 intentos de ingreso, si la contraseña es invalida, entonces el usuario o la aplicación deberá quedar bloqueada y se liberará por medio de propietario del recurso o por el responsable de área.

Cualquier desviación de los estándares de manejo de contraseña, deberá ser autorizada y negociada por el Gerente de Seguridad y/o informática.

4.5.11 Educación a usuarios en el manejo de contraseñas

La protección de los datos es algo esencial que los usuarios deban conocer, es decir que información esta almacenando, donde y como se pueden accesar y sí tiene código de seguridad. La educación al respecto será otorgada por el Gerente de Seguridad y/o informática.

Responsabilidad personal

Los usuarios deberán estar conscientes sobre la responsabilidad que tienen sobre su identificación y contraseña de usuario, por lo tanto, se sugiere el siguiente procedimiento para educación:

- Instrucciones sobre el manejo y uso de la seguridad en la computadora personal.
- Reglas del manejo de contraseña.
- Instrucciones de como firmar y terminar una sesión en el sistema.
- Regulaciones sobre los programas que se tengan en las computadoras personales(uso de programas autorizados únicamente, consideraciones de derechos de autor, etc.)
- Guías de como actuar en caso de un problema de Virus electrónico.
- Si existiera, como obtener apoyo del departamento de Soporte técnico.

4.6 Operación de los sistemas

Computadoras y redes de trabajo, serán operadas en un ambiente seguro y con programas autorizados. Todas las operaciones serán monitoreadas para el control de incidentes.

4.6.1 Medio ambiente

El número, tamaño y arreglo de las oficinas de informática, deberá permitirle a los empleados llevar a cabo las tareas de forma segura, confiable y en un período de tiempo apropiado.

Para la seguridad de los empleados y de los recursos de informática, las áreas de trabajo deberán estar acondicionadas con equipo de seguridad, tal como detectores de calor, agua y humo, alarmas de incendio, extinguidores de fuego, rutas de escape claramente marcadas.

4.6.2 Localización de los equipos

Los principales recursos de informática tales como servidores, equipos de comunicación, unidad de respaldo, archivos con cartuchos de respaldo deberán estar en oficinas seguras y con accesos especiales. Todo ingreso a las mismas deberá ser documentado.

En las organizaciones que trabajan con redes de trabajo extensas, el área deberá dividirse en varias zonas de seguridad, es decir, instalar un servidor por nivel del edificio, por ejemplo:

- Primer nivel servidor de archivos
- Segundo nivel servidor de sistemas de información
- Tercer nivel servidores para respaldo
- Cuarto nivel equipo de comunicación

4.6.3 Instalaciones y mantenimiento

Los responsables de los equipos deberán asegurarse de mantener un inventario del equipo instalado en sus respectiva áreas. Este inventario deberá ser chequeado cada vez que se adquiera o se cambie equipo.

El mantenimiento de los equipos se podrá llevar a cabo en las instalaciones propias o afuera de las mismas, dependiendo de la confidencialidad de la información que esté almacenada en los mismos. También, toda instalación y/o mantenimiento de equipo, será llevada a cabo por especialistas y bajo la supervisión del responsable correspondiente.

4.6.4 Equipo de análisis de redes

Equipo o programas para el análisis de tráfico en la red o en comunicaciones podrán ser empleado únicamente por personal autorizado.

4.7 Energía de calidad

Los problemas en el suministro de energía eléctrica afecta de manera significativa el rendimiento de una organización . Una interrupción puede implicar pérdidas de equipo y/o de información con un impacto económico alto.

Actualmente las organizaciones le han puesto mayor atención a este aspecto, debido al incremento del número de cargas sensibles en los sistemas de distribución, las cuales son una causa de degradación en la energía de calidad. Estos problemas de calidad de distribución se han agravado dado a una mayor utilización de equipo para procesamiento

de datos y comunicaciones, es decir, la demanda de energía ha crecido más rápido que la generación de la misma.

4.7.1 Definición de energía de calidad

La energía de calidad es la ausencia de interrupciones, sobretensiones, variaciones de voltaje suministrado y deformaciones producidas por armónicas en la red.

Existen tres elementos específicos que califican a la energía: Continuidad, frecuencia y voltaje del suministro.

Continuidad en el servicio

Esto se refiere a que la energía se encuentre disponible siempre que se necesite.

Rango de frecuencia

La energía de calidad se genera en forma de ondas senoidales, en teoría libre de armónicas, pero dependiendo de las cargas y características del sistema, se presentan distorsiones en la forma de las ondas. Sin embargo, usualmente la forma de las ondas es bastante razonable.

La frecuencia debe mantenerse en un valor nominal –60 ciclos por segundo (60 hertz) con variaciones muy pequeñas de frecuencia. En el sistema interconectado de una nación, el control de la frecuencia se maneja mediante sistemas electrónicos de verificación que lo mantienen con variaciones de centésimas de ciclo. Si la frecuencia varía a medio ciclo, se pone en riesgo la vida de los equipos y la estabilidad del sistema eléctrico.

Voltaje O tensión del suministro

Permite variaciones del +- 5%. En la medida que la calidad del servicio es buena, la variación se acerca a cero. Sin embargo se permite cierta tolerancia, ya que el funcionamiento de los sistemas eléctricos lleva implícitas ciertas variaciones que se procura mantener dentro de los rangos aceptables.

Las normas internacionales establecen una regulación de voltaje del +-5%, las organizaciones suministradoras en algunas ocasiones entregan valores menores o mayores, los cuales son intolerables para la operación de los equipos eléctricos y pueden acortar su vida. Además a lo largo de un día el voltaje no se mantiene estable, hay variaciones instantáneas con duración menor a un segundo y otras que duran varios minutos o más. Por ejemplo en horas de baja carga – en la madrugada -, el voltaje sube hasta un 10% o más, mientras que en horas de alta carga – 10:00 a.m. / 8:00 p.m. – el voltaje baja notablemente.

Las variaciones instantáneas de voltaje suelen no afectar a los usuarios, cuando el sistema está bien protegido. Sin embargo, los transitorios que implican sobrevoltajes con magnitudes muy altas, afectan gravemente a los equipos, tanto a los del administrador como los del usuario.

4.7.2 Principales problemas en la calidad de la energía

Interrupciones momentáneas de energía, que algunas veces duran varias horas, parpadeos, picos y caídas de voltaje así como ruidos.

Las variaciones de voltaje en las líneas de suministro son causadas por: desconexión y conexión en la red, capacidad limitada en las sub-estaciones, correcciones del factor de potencia, disparos de interrupciones de circuitos y fusibles quemados. Los períodos de bajo voltaje resultan por reducciones programadas por la organización de energía eléctrica y ocurren cuando la demanda de energía se acerca a la capacidad disponible de la distribución.

Las fluctuaciones de voltaje pueden ser causadas también por una demanda fuerte y repentina de energía, originada por la utilización de altas cargas de fuerza por parte de grandes industrias o para arrancar enormes motores.

Por otro lado, los apagones generalmente son provocados por disturbios en los elementos constitutivos del sistema (fallas en las líneas, transformadores, generados); por descargas atmosféricas inesperadas o cortos circuitos que, cuando ocurren, duran desde fracciones de segundos hasta días. Asimismo, las restricciones de energéticos como agua o petróleo, limitan la producción de energía eléctrica.

4.7.3 Causas de los problemas en el suministro de energía

Naturales	No naturales
Tormenta eléctrica	Apagón
Lluvia	Pico de voltaje
Viento	Caída de voltaje

Polvo	Pérdida de fase
Nieve	Sobrecarga
Granizada	Corto circuito
Inundación	Ruidos eléctricos
Terremoto	Conexión y desconexión de la red
Tornado	Corrección del factor de potencia
Huracán	Conexión y desconexión de cargas
Helada	Apertura de interruptor
Humedad	Falla del transformador
Salinidad	Falta de equipo de generación
	Rotura de líneas
	Fusiles quemados
	Mantenimiento
	Suspensión del servicio
	Accidente

En conclusión, se puede señalar que la calidad de la energía eléctrica es el resultado de una atención continua por parte de las organizaciones proveedoras, pero también por parte de los usuarios. Recuerde que los procesos son tanto más eficientes cuanto mejor es la calidad de la energía eléctrica.

Como se mencionó anteriormente, las fallas, distorsiones y desequilibrios en las líneas eléctricas comerciales (transmisión, distribución y suministro de energía eléctrica) son las causas principales de los problemas de los equipos.

Sin embargo, un problema más grave se refiere al desperdicio de energía y al descuido y mal manejo que los usuarios le dan a nuestros equipos, por lo que muchas veces los costos de la energía son más altos. Sin embargo, las organizaciones pueden minimizar los problemas de energía si toman en cuenta lo siguiente:

Una instalación eléctrica adecuada debe tener conexiones a tierra para drenar la corriente cuando se produzcan fenómenos transitorios o cortos circuitos. Además, el sistema de tierras protege a las personas de posibles sobre voltajes que pueden ser mortales.

Los edificios que no disponen de un diferencial o una red de tierra, necesitan interrupciones diferenciales de alta sensibilidad.

Los picos, sobretensiones y perturbaciones de voltaje pueden resolverse con supresores de sobre tensión, únicamente para proteger los recursos de informática. Así mismo, los capacitores, compensadores, sensores de voltaje y pararrayos en los edificios también ayudan a compensar estas variaciones.

La baja o alta tensión puede controlarse con reguladores de voltaje, sin embargo, estos no son respaldo durante un apagón total.

Los sistemas sofisticados sensibles a las armónicas requieren filtros que las corrijan.

Los sistemas de energía eléctrica ininterrumpida (UPS), proveen protección contra los tiempos muertos ocasionados por fallas y distorsiones eléctricas dañinas en las líneas de abastecimiento comercial, asegurando la continuidad de las operaciones computarizadas y las telecomunicaciones sin sufrir interrupciones. Estos sistemas, ya sean electromecánicos o alimentados por baterías, mantienen el abastecimiento de energía.

Los sistemas de energía eléctrica ininterrumpida (UPS) alimentados por baterías requieren de equipo para cargarlas, mantenimiento y reposición de baterías. Además, presentan contratiempos como: agotamiento de energía, envejecimiento, peligros de explosión y contaminación.

Las fábricas que emplean cargas muy grandes (megawatts) para hacer funcionar sus equipos –por ejemplo, un horno eléctrico, o las organizaciones que requieren una continuidad obligatoria del servicio eléctrico -, suelen instalar alimentaciones redundantes, más de un alimentador o inclusive más de una línea de alta tensión. Con eso, en la mayoría de los procesos que requieren servicio continuo, la interrupción se supera, pues el sistema automático de transferencia garantiza la continuidad. Además, de que el equipo de control se alimente con una fuente ininterrumpida (UPS)

En las zonas arboladas puede usarse cable semiaislado para aislar los conductores de media tensión. Esta acción disminuye su vulnerabilidad al contacto con las ramas de los árboles y el efecto que la lluvia y el viento tienen sobre los alimentadores.

Existe también un concepto muy importante que ha logrado buenos resultados en las organizaciones que lo han instalado: La generación independiente de energía o auto-generación, la cual fue impulsada desde hace varios años. Este proceso implica la generación de energía por parte de los usuarios capaces de hacerlo, aquellos que utilizan recursos energéticos –como el vapor -, lo que les permite generar simultáneamente a los procesos de trabajo que realizan. De esta manera, los hospitales, hoteles, baños públicos, ingenios, papeleras y cartoneras, además de ahorrar energía y no desperdiciar su capacidad energética, pueden generar su propia energía y garantizar su calidad.

4.8 Manejo de las operaciones

Cuando sean asignadas tareas al personal, la segregación de las siguiente funciones deberá ser considerada:

- Desarrollo de sistemas
- Operación de sistemas
- Autorización acceso de usuarios
- Auditoría de funciones
- Administración de seguridad

4.8.1 Operación de los sistemas

Solamente programas que han sido autorizados por el propietario de recurso podrán ser utilizados. Programas de origen desconocido no serán ejecutados.

Los ambientes de operación deberán ser separados, es decir, deberá existir un ambiente para pruebas y otro ambiente para producción. La información que se encuentra en el sistema que está en producción, nunca se deberá utilizar como prueba.

Los responsables de los sistemas de información y/o aplicaciones de usuarios, deberán ejecutar sus rutinas de respaldo. También deberán generar algunas pruebas para determinar que los mismos han sido copiados al medio utilizado correctamente.

4.8.2 Operación en ambiente productivo

Sistemas y aplicaciones para ambiente productivo, serán cambiados únicamente por el responsable del mismo. Cada cambio será documentado de tal forma que si es necesario reversar el cambio, esto sea posible.

Para cada cambio se deberá hacer por escrito de parte del responsable, así como la aceptación de los cambios realizados. El formulario de aceptación de cambios deberá incluir una sección de “pruebas”. Este formulario deberá estar firmado por el responsable del sistema y la persona que realizó el cambio.

Este formulario se archivará en el lugar donde se tienen los demás formularios de cambios requeridos y aceptados, con el propósito de llevar control de versiones.

Cuando se realice un cambio al sistema, éste se deberá notificar a todos los usuarios involucrados, así como en que momento entrará a funcionar el mismo. Esto se deberá hacer con anticipación.

Tomar nota que los archivos de documentación deberán estar almacenados en un lugar seguro y que cuente con alarmas de detección de humo/fuego.

4.8.3 Medios de almacenamiento

Impresoras que tienen como tarea la impresión de reportes de carácter confidencial, se deberán administrar de tal forma que solamente personal autorizado tenga acceso a las mismas. Cintas, Cartuchos, discos compactos y otros medios de almacenamiento de datos, deberán almacenarse en cuartos con protección y preferiblemente fuera del edificio donde operan los servidores principales.

Cintas, Cartuchos, discos compactos y otros medios de almacenamiento de datos que ya no se van a utilizar más, deberán ser destruidos en su totalidad.

4.8.4 Monitoreo de operaciones

Operaciones en Servidores, sistemas Multi-Usuarios, deberán ser monitoreados con el propósito de detectar anomalías en los mismos. Ejemplo: Violación de accesos, usuarios bloqueado por 3 intentos fallidos, Contraseña inválida, mal manejo de privilegios.

Cuando se ha detectado alguna anomalía en el sistema, se deberá realizar un reporte describiendo el incidente y luego tener una reunión con el responsable del mismo, la

persona afectada y el encargado de la seguridad. Esto con el propósito de detectar posible debilidades en la seguridad.

CAPÍTULO 5

5 Colaboración de informática con otras organizaciones

La colaboración con otras organizaciones e instituciones en el área de informática causa riesgos los cuales se deben de mantener dentro de los limites tomando prevenciones con adecuada seguridad. Este es el caso cuando:

- Personas ajenas trabajan con computadoras de la organización
- Información de la organización que se procesa en sistemas ajenos.

5.1 Responsabilidad en la colaboración

Los jefes de departamento de la organización son quienes toman la decisión de la colaboración en informática con otras instituciones. Dicha decisión depende de asuntos del negocio, cuestiones legales o gubernamentales.

5.2 Autorización para la colaboración

Programas y datos serán disponibles a otras organizaciones únicamente con la autorización del propietario de la información.

5.3 Reglas de responsabilidad claras

Para cada aplicación un empleado especifico de la organización debe ser el responsable de la colaboración con otras organizaciones. Usualmente el empleado responsable de la organización el gerente o jefe de departamento que tiene el principal interés de negocio con la otra organización .

5.4 Obligación de confidencialidad

Debe existir un convenio con la otra organización de mantener bajo estricta confidencialidad la información que se le proporcione.

5.5 Comunicación de computadoras

Cuando se planean y se construyen los enlaces para la comunicación, el propietario de la red de la organización debe de estar seguro que las personas de otras organizaciones sólo tendrán accesos a los sistemas predeterminados. Los administradores del sistema y de la red deben de garantizar que sólo se permitirán conexiones legítimas.

5.6 Consideración de riesgos en la comunicación

Los administradores y especialista de la red deben de considerar todos los riesgos que puedan poner en peligro la confidencialidad de la información. Adicionalmente la información podrá ser enviada encriptada o transmitida con contraseña.

5.7 Usuarios externos a la organización en los sistemas

Autorización individual

Una fiable identificación de cada usuario es un elemento importante en la seguridad, por lo tanto cada usuario necesita recibir una contraseña individual. Los accesos y permisos pueden ser asignados por grupo, y luego hacer al usuario participe de un grupo.

Accesos y permisos restringidos

Los usuarios deben de recibir los accesos y permisos a los programas e información que necesitan para realizar su trabajo. Todas las autorizaciones de accesos a las personas ajenas a la organización deben de tener una fecha de expiración y para ser prolongada se deberá volver a solicitar su aprobación. Las autorizaciones para otras organizaciones deben ser restringidas por aplicación, horario y fecha.

5.8 Medidas de seguridad para procesar información en instalaciones ajenas

Para procesar información en instalaciones ajenas deben considerarse los siguientes aspectos de seguridad.

- Protección física para los sistemas de computación a ser utilizados
- Reglas de acceso a los lugares donde están las computadoras y los sistemas
- Seguridad de los programas e información e identificación de usuarios
- Protección contra accesos no autorizados
- Registros de auditoría para los sistemas ejecutados
- Plan de recuperación en caso de desastres.

CAPÍTULO 6

6 Plan de contingencias

El Plan de contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos los equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que se hará un análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas las medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

Al trabajar sobre la base de un ejemplo que presupone un incendio en el local, el cual ha dejado sin equipos de cómputo y sin los archivos magnéticos (programas y datos) contenidos en dichos equipos y en las oficinas del local.

Hay dos ámbitos que se van analizar. El primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas. El segundo, el control, esto

es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está operativo y actualizado.

Haciendo un esquema, el Plan de Contingencias abarcará los siguientes aspectos:

6.1 Plan de reducción de riesgos(plan de seguridad)

Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

6.1.1 Análisis de riesgos

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección de la Información en análisis, versus el costo de volverla a producir (reproducir).

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que suceda cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

El análisis de riesgos supone responder a preguntas del tipo:

¿Qué puede ir mal?

¿Con qué frecuencia puede ocurrir?

¿Cuáles serían sus consecuencias?

¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

¿Qué se intenta proteger?

¿Cuál es su valor para uno o para la organización?

¿Frente a qué se intenta proteger?

¿Cuál es la probabilidad de un ataque?

A continuación se muestra un ejemplo de cómo se realiza una evaluación de riesgos.

El o los responsables de la oficina de informática se sentarán con los responsables de las áreas usuarias y realizarán el siguiente conjunto de puntualizaciones:

¿A qué riesgos en la seguridad informática se enfrenta la Institución?

- Al fuego, que puede destruir los equipos y archivos.
- Al robo común, llevándose los equipos y archivos.
- Al vandalismo, que dañen los equipos y archivos.
- A fallas en los equipos, que dañen los archivos.

- A equivocaciones, que dañen los archivos.
- A la acción de virus, que dañen los equipos y archivos.
- A terremotos, que destruyen el equipo y los archivos.
- A accesos no autorizados, filtrándose datos no autorizados.
- Al robo de datos, difundiéndose los datos sin cobrarlos.
- Al fraude, desviando fondos merced a la computadora.

Esta lista de riesgos que se puede enfrentar en la seguridad, es bastante corta. La Institución deberá profundizar en el tema para poder tomar todas las medidas del caso.

Luego de elaborar esta lista, el personal de la organización estará listo para responder a los efectos que estos riesgos tendrán para su Institución.

¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

¿ Al fuego, que puede destruir los equipos y los archivos?

¿Cuenta con protección contra incendios?

¿Se cuenta con sistemas de aspersión automática?

¿Diversos extintores?

¿Detectores de humo?

¿Los empleados están preparados para enfrentar un posible incendio.?

A un robo común, llevándose los equipos y archivos

¿En que tipo de vecindario se encuentra la institución?

¿Hay venta de drogas?

¿Las computadoras se ven desde la calle?

¿Hay personal de seguridad en la institución?

¿Cuántos vigilantes hay?

¿Los vigilantes, están ubicados en zonas estratégicas?

Al vandalismo, que dañen los equipos y archivos

¿Existe la posibilidad que un ladrón desilusionado o frustrado cause daños?

¿Hay la probabilidad que cause algún otro tipo de daño intencionado?

A fallas en los equipos, que dañen los archivos

¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?

¿Cuáles son las condiciones actuales del hardware?

¿Es posible predecir las fallas a que están expuestos los equipos?

A equivocaciones que dañen los archivos

¿Cuánto saben los empleados de computadoras o redes?

¿Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?

¿Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

A la acción de virus, que dañen los archivos

¿Se prueba software en la oficina sin hacerle un examen previo?

¿Está permitido el uso de disquetes en la oficina?

¿Todas las máquinas tienen unidades de disquetes?

¿Se cuentan con procedimientos contra los virus?

A terremotos, que destruyen los equipos y archivos

¿La Institución se encuentra en una zona sísmica?

¿El edificio cumple con las normas antisísmicas?

Un terremoto,

¿Cuánto daño podría causar?

A accesos no autorizados, filtrándose datos importantes

¿Cuánta competencia hay para la organización?

¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?

¿El módem se usa para llamar fuera y también se puede utilizar para comunicarse hacia dentro?

¿Se cuenta con Sistemas de Seguridad en el Correo Electrónico o Internet?

Al robo de datos; difundiéndose los datos

¿Cuánto valor tiene actualmente las Bases de Datos?

¿Cuánta pérdida podría causar en caso de que se hicieran públicas?

¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?

La lista de sospechosos

¿Es amplia o corta?

¿ Al fraude, desviando fondos merced a la computadora?

¿Cuántas personas se ocupan de la contabilidad de la Institución?

¿El sistema de contabilidad es confiable?

Las personas que trabajan en el departamento de contabilidad, ¿qué tipo de antecedentes laborales tienen?

¿Existe acceso al sistema contable desde otros sistemas o personas?

Para cada riesgo, se debe determinar la probabilidad del factor de riesgo. Como ejemplo se mencionan algunos factores de riesgo:

- Factor de riesgo muy bajo
- Factor de riesgo bajo

- Factor de riesgo medio
- Factor de riesgo alto
- Factor de riesgo muy alto

Luego se efectuará un resumen de los riesgos ordenados por el factor de riesgo de cada uno. Ejemplo:

6.1.2 Análisis de fallas en la seguridad

Esto supone estudiar las computadoras, su software, localización y utilización con el objeto de identificar los resquicios en la seguridad que pudieran suponer un peligro. Por ejemplo, si se instala una computadora personal nueva, para recibir informes de inventario desde otras PC´s vía módem situados en lugares remotos, y debido a que el módem se ha de configurar para que pueda recibir datos, se ha abierto una vía de acceso al sistema informático. Habrá que tomar medidas de seguridad para protegerlo, como puede ser la validación de la clave de acceso.

6.1.3 Protecciones actuales

Generales: ¿Se hace una copia casi diaria de los archivos que son vitales para la Institución?

Robo común: ¿se cierran las puertas de entrada y ventanas?

Vandalismo: ¿se cierra la puerta de entrada?

Falla de los equipos: ¿se tratan con cuidado, se realiza el mantenimiento de forma regular, no se permite fumar, está previsto el préstamo de otros equipos?

Daño por virus: ¿todo el software que llega se analiza en un sistema utilizando software antivirus? ¿Los programas de dominio público y de uso compartido (Shareware), sólo se usan si proceden de una fuente fiable?

Equivocaciones: ¿Los empleados tienen buena formación?

Acceso no autorizado: ¿Se cierra la puerta de entrada?

Robo de datos: ¿Se cierra la puerta principal?

Fuego: ¿En la actualidad se encuentra instalado Sistemas contra incendios, extinguidores, en sitios estratégicos y se brinda entrenamiento en el manejo de los sistemas o extinguidores al personal, en forma periódica?

6.2 Plan de recuperación de desastres

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, debe ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la organización

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

6.2.1 Actividades previas al desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.

Podemos detallar las siguientes Actividades Generales:

Establecimiento del plan de acción.

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

- Sistemas e Información.
- Equipos de Cómputo.
- Obtención y almacenamiento de los Respaldos de Información.
- Políticas (Normas y Procedimientos de Copia de respaldo).

Sistemas e Información. La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha de las operaciones.

La relación de Sistemas de Información deberá detallar los siguientes datos :

- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).
- La Dirección (Gerencia, Departamento, etc.) que genera la información base (el «dueño» del Sistema).
- Las unidades o departamentos (internos/externos) que usan la información del Sistema.
- El volumen de los archivos que trabaja el sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del Sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.

El nivel de importancia estratégica que tiene la información de este sistema (medido en horas o días que la institución puede funcionar adecuadamente, sin disponer de la

información del sistema). Equipamiento mínimo necesario para que el sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).

Actividades a realizar para volver a contar con el Sistema de Información (actividades de restauración de información).

Con toda esta información se deberá de realizar una lista priorizada de los sistemas de información necesarios para que la organización pueda recuperar su operatividad perdida en el desastre (contingencia).

Equipos de Cómputo. Aparte de las normas de seguridad que se verán en los capítulos siguientes, hay que tener en cuenta :

Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar de color rojo a los Servidores, color amarillo a las PC's con Información importante o estratégica y color verde a las PC's de contenidos normales.

Tener siempre actualizada una relación de PC's requeridas como mínimo para cada sistema permanente de la institución (que por sus funciones constituyen el eje central de los servicios informáticos de la organización), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

Formación de equipos operativos

En cada unidad operativa de la Institución, que almacene información y sirva para la operatividad institucional, se deberá designar un responsable de la seguridad de la información de su unidad. Pudiendo ser el jefe de dicha área operativa.

Sus labores serán:

- Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
- Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
- Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
- Supervisar procedimientos de respaldo y restauración.
- Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
- Coordinar líneas, terminales, módem, otros aditamentos para comunicaciones.
- Establecer procedimientos de seguridad en los sitios de recuperación.

- Organizar la prueba de hardware y software.
- Ejecutar trabajos de recuperación.
- Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
- Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
- Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
- Participar en las pruebas y simulacros de desastres

Formación de Equipos de Evaluación (auditoría de cumplimiento de los procedimientos sobre Seguridad).

Esta función debe ser realizada de preferencia por personal de Inspectoría, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos :

Revisar que las normas y procedimientos con respecto a copia de respaldo y seguridad de equipos y data se cumplan.

Supervisar la realización periódica de las copias de respaldo, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la organización, y las copias de respaldo realizadas.

Informar de los cumplimientos e incumplimientos de las normas, para las acciones de corrección respectivas.

6.2.2 Actividades durante el desastre

Una vez presentada la contingencia o siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

Plan de emergencias.

En este plan se establecen las acciones se deben realizar cuando se presente un siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro :

- Durante el día.
- Durante la Noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar :

- Vías de salida o escape.
- Plan de evacuación del personal.

- Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)

- Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)

- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

Formación de equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades, para salvar los equipos señalados en el párrafo bajo el nombre de plan de emergencias.

Entrenamiento.

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los

planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

6.2.3 Actividades después del desastre.

Después de ocurrido el siniestro o desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el plan de acción.

Evaluación de daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se estén afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la institución con la cual se tiene el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

Priorización de actividades del plan de acción.

Toda vez que el plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el plan dará la lista de las actividades que se deben

realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de la institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

Ejecución de actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el plan de acción (6.2.1.1). Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del sistema de información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio del sistema e imagen institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

Evaluación de resultados.

Una vez concluidas las labores de recuperación de los sistemas que fueron afectados por el siniestro, se debe de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o

entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

Retroalimentación del plan de acción

Con la evaluación de resultados, se debe de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no haber tenido la organización el plan de contingencias llevado a cabo.

CAPÍTULO 7

7 Alta disponibilidad

El concepto de alta disponibilidad se establece como la implementación de sistemas que proporcionan:

- Disponibilidad de servicios cuando se requieren.
- Minimización de los tiempos en que el sistema se encuentra fuera de servicio.
- Implementaciones para prevenir la falla de servicios.
- Tolerancia a fallas

La disponibilidad de los servicios críticos en una red de computadoras se ven afectados por tiempos muertos programados y no programados. Aunque programar el tiempo muerto para el mantenimiento y las mejoras del sistema es inevitable, son fatales a los servicios que se consideran no interrumpidos. Además, el tiempo muerto no programado es imprevisible y debe ser evitado. Los errores humanos, las fallas del sistema operativo, las fallas del hardware y las fallas de la red son generalmente la causa de la mayoría de los tiempos muertos no programados.

Para describir los métodos para prevenir estos incidentes, primero se deben entender las definiciones de los niveles de la disponibilidad:

- Disponibilidad normal de un sistema

- Alta disponibilidad de un sistema

- Tolerancia a fallas

Disponibilidad normal de un sistema

Esto se define como el uso común que tiene una computadora tanto en su hardware como en su software y que no cuenta con un sistema de redundancia o herramientas que le permitan recuperarse ante una falla. Estos requieren de intervención manual humana para identificar, corregir y/o reparar los componentes dañados para luego iniciar de nuevo el sistema.

Alta disponibilidad de un sistema

Se define como la dotación física redundante de componentes de hardware, manejados por software que proporciona procedimientos de detección y corrección de fallas, con el propósito de maximizar la disponibilidad de los servicios y aplicaciones de carácter críticos proporcionados por el sistema.

Estos sistemas no requieren ninguna intervención manual humana para identificar un componente dañado, sino que ejecutan un procedimiento para evitar una falla en el sistema y ejecutan procedimientos de corrección. Esta configuración reduce al mínimo la posibilidad de pérdida de los datos e interrupción del servicio.

Existen 2 modelos de alta disponibilidad:

- Replicación de servicios

- Failover.

Modelo replicación de los servicios:

Este modelo utiliza aplicaciones distribuidas y bases de datos distribuidas en los servidores múltiples en el ambiente de LAN/WAN donde los datos se replican a algunos o a todos los servidores. Cuando ocurre una falla en el servidor, los datos y las aplicaciones son accesibles desde un servidor alterno.

Modelo de failover

Este modelo utiliza las configuraciones de redundancia física del servidor, en las cuales un servidor tiene el papel activo para los datos y las aplicaciones que se están ejecutando, mientras que el otro es un servidor de reserva que vigila el estado del servidor activo.

Cuando el servidor de reserva detecta una falla en el servidor activo, ya sea falla de hardware o de software, éste asume el control y la identidad del servidor activo.

Tolerancia a fallas

El manejo de fallas está integrado y se convierte en una función del sistema operativo. Estos sistemas tienen respuesta espontánea y completamente automática a las fallas del sistema y proporcionan servicios ininterrumpidos, ya que hay duplicidad de recursos, aunque es una solución costosa, pero efectiva cuando se requiere de servicios continuos.

Redundancia de equipo

Actualmente las empresas productoras de equipo de computación han desarrollado el concepto de alta disponibilidad en los Servidores, Clustering para asegurar la máxima

disponibilidad en aplicaciones de misión crítica, Tolerancia a fallas implementando Arreglos de discos (RAID) fuentes de poder redundantes para proteger sus sistemas a posibles fallas eléctricas. Los requerimientos de disponibilidad dependeran del tipo de aplicaciones que corren en lo servidores. A continuación se muestra una tabla que indica el nivel de disponibilidad y su clasificación económica.

Niveles de Disponibilidad Requeridos		
Aplicaciones de misión-crítica que requieren tolerancia a fallas. Aplicación de administración-crítica que requieren cierto nivel de alta disponibilidad. Aplicaciones convenientes que no requieren alta disponibilidad.	Costo más Alto Costo más bajo	Sistema de intercambio comercial, control de tráfico aéreo. Procesamiento de transacciones, manejo de base de datos. Correo electrónico. Compartimento de archivos de empresas. Respaldo de trabajos y servicios de impresión.

7.1 Clusternig

Es un grupo independiente de servidores que se presentan ante la red como un sistema único. En la gráfica 7.1 se puede observar un ejemplo de este esquema de información compartida en una red privada.

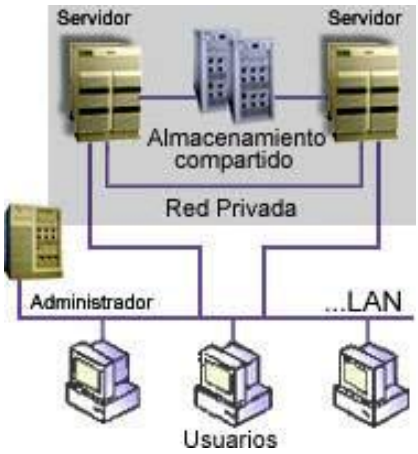


Figura 7.1

Características

- Múltiples servidores independientes funcionando como un sistema servidor único.
- Los servidores tienen un nombre común.
- Los servidores están disponibles a todas las máquinas conectadas a la red.
- Pueden tolerar fallas de componentes. Se pueden agregar componentes sin interrumpir a los usuarios.

Ventajas

Alta disponibilidad de recursos: Las aplicaciones Cliente/Servidor recaen en la disponibilidad de los servicios de la red. Estos servicios son proporcionados por los recursos. Si los recursos no están disponibles debido a fallas en aplicaciones o fallas del hardware, el trabajo del usuario es interrumpido. Clustering incrementa la disponibilidad de estos recursos del servidor.

Escalabilidad: Recursos de aplicación, de entrada/salida y CPU pueden ser añadidos, para expandir eficientemente la capacidad del sistema sin interrupción del servicio al usuario. Esto se traduce en un acceso confiable a recursos del sistema e información, así como protección de la inversión de los recursos de hardware y software.

Administración centralizada: En un ambiente de servidores comunes, se utilizan varias herramientas administrativas para identificar los servidores en la red, monitorear sus contenidos y actividades. Sin embargo en un ambiente de cluster, la administración de aplicaciones y servicios puede ser centralizada, a través del uso de una herramienta de administración y monitoreo de redes.

7.2 Arreglos de discos

Un arreglo de discos es un subsistema que consiste de múltiples discos bajo el mando de un controlador de arreglos. Este controlador es una tarjeta inteligente de alto rendimiento con capacidades de control de RAID, proporcionando una solución efectiva en ambientes que requieren un buen rendimiento, protección de la información, confiabilidad, flexibilidad y disponibilidad.

Funciones

- Incrementar la disponibilidad de la información.
- Mejorar la capacidad de almacenamiento.
- Permitir una flexibilidad en la ejecución mediante la distribución selectiva de la información en múltiples discos duros.

RAID (Redundant Array of Independent Disks)

Es una técnica que permite agrupar cierto número de discos para propósitos de disponibilidad, proporcionando la redundancia necesaria para la protección de información y que a veces provee ventajas en el rendimiento. Muchas configuraciones de arreglos de discos son posibles, dependiendo de los requerimientos del usuario final.

7.2.1 RAID Nivel 0

Este tipo de arreglo utiliza una técnica llamada "striping", la cual distribuye la información en bloques entre los diferentes discos. Es el único nivel de RAID que no duplica la información, por lo tanto no se desperdicia capacidad de almacenamiento. Se requieren mínimo dos discos.

Ventajas

RAID-0 permite accesar más de un disco a la vez, logrando una tasa de transferencia más elevada y un rápido tiempo de acceso. Por no utilizar espacio en información redundante, el costo por Megabyte es menor.

Ambientes donde implementarlo:

Es una buena alternativa en sistemas donde sea más importante el rendimiento que la seguridad de los datos. Es decir ambientes que puedan soportar una pérdida de tiempo de operación para poder reemplazar el disco que falle y reponer toda la información.

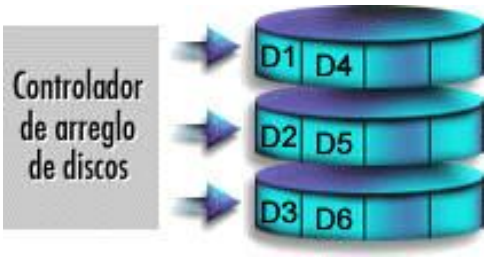


Figura 7.2
Fuente:http://www.hp.com

7.2.2 RAID Nivel 1

Este nivel de RAID usa un tipo de configuración conocido como "mirroring", ya que la información de un disco es completamente duplicada en otro disco. Así mismo, también se puede duplicar el controlador de disco (duplexing). Se desperdicia el 50% de la capacidad y sólo maneja dos discos.

Ventajas

Se protege la información en caso de falla tanto del disco como del controlador (en caso de duplex), ya que si un disco suspende su operación el otro continua disponible. De este modo se evita la pérdida de información y las interrupciones del sistema debido a fallas de discos.

Ambientes donde implementarlo:

RAID-1 está diseñado para sistemas donde la disponibilidad de la información es esencial y su reemplazo resultaría difícil y costoso (más costoso que reponer el disco en sí). Típico en escrituras aleatorias pequeñas con tolerancia a fallas. El problema de este tipo de arreglos es el costo que implica duplicar los discos.

Figura 7.3
Fuente:http://www.hp.com

7.2.3 RAID Nivel 3

Conocido también como "striping con paridad dedicada", utiliza un disco de protección de información separado para almacenar información de control codificada. Esta información de control codificada o paridad proviene de los datos almacenados en los discos y permite la reconstrucción de la información en caso de falla. Se requieren mínimo tres discos y se utiliza la capacidad de un disco para la información de control.

Ventajas

RAID-3 proporciona una alta disponibilidad del arreglo, así como una tasa de transferencia elevada, mejorando de ese modo el rendimiento del sistema.

Ambientes donde implementarlo

Es típico para transferencia larga de datos en forma serial , tal como aplicaciones de imágenes o vídeo.

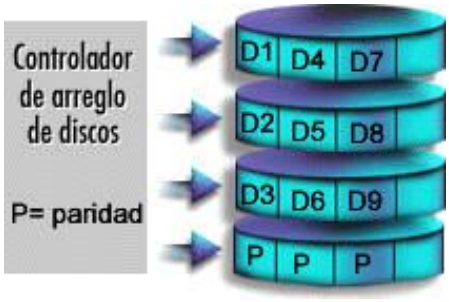


Figura 7.4
Fuente:http://www.hp.com

7.2.4 RAID Nivel 5

Este nivel de RAID es conocido como "striping con paridad distribuida", ya que la información se reparte en bloques como RAID-0, pero un bloque de cada disco se dedica a la paridad. Es decir la data codificada se añade como otro sector que rota por los discos igual que los datos ordinarios. Se requieren mínimo tres discos.

Ventajas

Es el esquema de protección de información más usado comúnmente, ya que proporciona un buen rendimiento general con una mínima pérdida de capacidad. Además el sistema tiene suficiente redundancia para ser tolerante a fallos.

Ambientes donde implementarlo

Es recomendable para aplicaciones intensas de entrada/salida y de lectura/escritura, tal como procesamiento de transacciones.

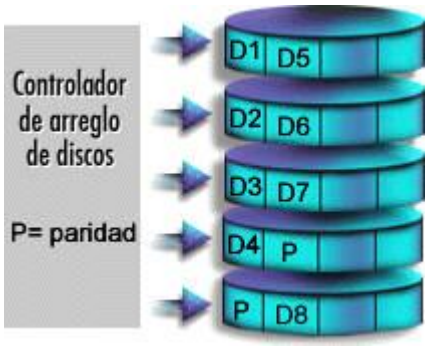


Figura 7.5
Fuente: http://www.hp.com

7.2.5 RAID Nivel 10

Es un nivel de arreglo de discos, donde la información se distribuye en bloques como en RAID-0 y adicionalmente, cada disco se duplica como RAID-1, creando un segundo nivel de arreglo. Se conoce como "striping de arreglos duplicados". Se requieren, dos canales, dos discos para cada canal y se utiliza el 50% de la capacidad para información de control.

Ventajas

Este nivel ofrece un 100% de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante.

Ambientes donde implementarlo

Ideal para sistemas de misión crítica donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea. Es apropiado también en escrituras aleatorias pequeñas.

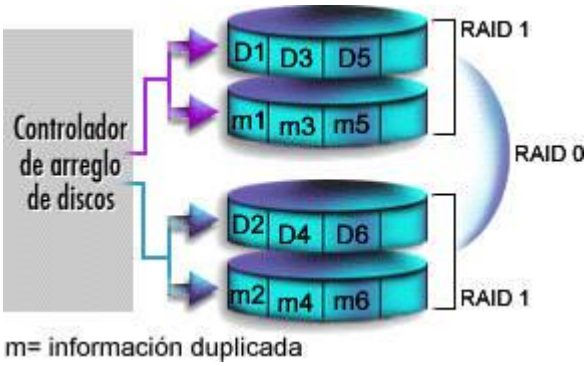


Figura 7.6
Fuente: http://www.hp.com

7.2.6 RAID Nivel 30

Se conoce también como "striping de arreglos de paridad dedicada". La información es distribuida a través de los discos, como en RAID-0, y utiliza paridad dedicada, como RAID-3 en un segundo canal. Requiere mínimo seis discos.

Ventajas

Proporciona una alta confiabilidad, igual que el RAID-10, ya que también es capaz de tolerar dos fallas físicas de discos en canales diferentes, manteniendo la información disponible.

Ambientes donde implementarlo

RAID-30 es el mejor para aplicaciones no interactivas, tal como señales de vídeo, gráficos e imágenes que procesan secuencialmente grandes archivos y requieren alta velocidad y disponibilidad.

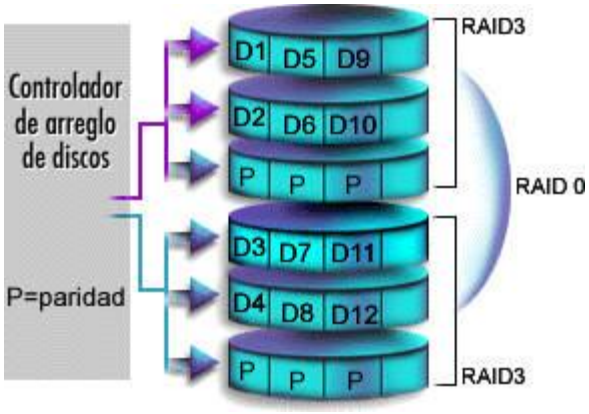


Figura 7.7
Fuente: http://www.hp.com

7.2.7 RAID Nivel 50

Con un nivel de RAID-50, la información se reparte en los discos y se usa paridad distribuida, por eso se conoce como "striping de arreglos de paridad distribuida". Se requieren mínimo seis discos.

Ventajas

Se logra confiabilidad de la información, un buen rendimiento en general y además soporta grandes volúmenes de datos. Igualmente, si dos discos sufren fallas físicas en diferentes canales, la información no se pierde.

Ambientes donde implementarlo

RAID-50 es ideal para aplicaciones que requieran un almacenamiento altamente confiable, una elevada tasa de lectura y un buen rendimiento en la transferencia de datos.

A este nivel se encuentran aplicaciones de oficina con muchos usuarios accesando pequeños archivos, al igual que procesamiento de transacciones.

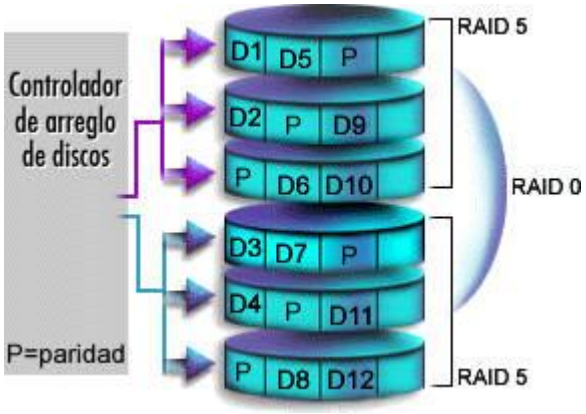


Figura 7.8
Fuente:http://www.hp.com

7.3 Fuentes de poder redundantes

Consiste de varios módulos de potencia redundantes (Redundant Power Modules-RPM), los cuales proporcionan balance de potencia y redundancia en caso de falla. Un subsistema RPS protege a un Servidor en caso que falle una fuente de poder.

Características

La carga de corriente es compartida y cada fuente de poder funciona a una capacidad reducida bajo condiciones normales, para configuraciones redundantes.

La falla de alguna fuente, ocasiona que las otras incrementen su salida rápidamente, antes que el sistema experimente interrupción de potencia.

Redundant Power Modules-RPM

- Cada RPM es idéntico y funciona independiente y cooperativamente para suministrar al sistema potencia balanceada.

- Cada módulo se puede cambiar de inmediato

- 90-240VAC (Voltios AC) autorango, es decir el módulo es capaz de adaptarse al voltaje en ese rango.

- Tiene un LED indicador del estado del módulo.

- Tiene una cerradura.

- Ventilador de velocidad variable.

- Conectores posteriores que proporcionan corriente DC e información del estado del I2C (Inter Integrated Circuit), lo cual permite administración remota a través de algún sistema de administración de Red.

Figura 7.9
Fuente: http://www.hp.com

CAPÍTULO 8

8 Respaldo de la información

Para prevenir la pérdida de información contenida en cualquier medio de almacenamiento es necesario realizar copias de respaldo.

8.1 Riesgos que se presenta en el almacenamiento de información

En el almacenamiento de información debe tenerse siempre en consideración los riesgos que pueden presentarse con respecto a la seguridad de la información.

A continuación se detallan las posibles eventualidades que pueden producir la pérdida o deterioro de los datos o información que están contenidos en los dispositivos de almacenamiento:

- Se pueden malograr uno o varios sectores en el disco trayendo consigo la pérdida de los datos de un archivo. Con la ayuda de utilitarios estos sectores se marcan como defectuosos, para evitar que se sigan grabando los datos en ellos.

- Se puede borrar un archivo o más en forma accidental, los cuales pueden como no ser recuperados, estando sujetos al utilitario empleado en la recuperación y de los sectores disponibles que tenga el disco.

- Se puede reformatear accidentalmente un disco. En este caso existen utilitarios que anulan los daños de un formateo siempre y cuando el anterior se haya hecho de manera simple.

- Una falla en la alimentación de corriente en el momento en que se está salvando un archivo puede provocar la pérdida en la memoria y en el disco.

- Se puede copiar un archivo sobre otro diferente pero que tiene el mismo nombre o alterar un archivo de forma irreversible.

- Se pueden borrar archivos que se desean guardar en el momento de maximizar el espacio en disco y aparezca un mensaje de disco lleno.

- Se puede dar un comando equivocado a un programa de utilidad de gestión de disco y borrar ramas completas del árbol de directorios.

- Se puede perder información de un disco si al sistema ha entrado virus informáticos.

- En últimas circunstancias la información se puede perder si se pierde la máquina por causas de robo o incendio.

8.2 Requerimientos para un copia de respaldo

Para crear un buen sistema de copias de respaldo se debe tener en cuenta los siguientes factores:

8.2.1 Equipo frente a programas

Aunque el equipo de informática (unidades de cinta, unidades de cartuchos removibles, discos) es importante, la flexibilidad y fiabilidad de las copias de respaldo dependen también de los programas, los cuales determinan si los requerimientos del usuario pueden ser satisfechos o no.

8.2.2 Programas de copias de respaldo

Deben tener flexibilidad y un buen sistema de corrección de errores para evitar que se copien originales dañados sobre copias de respaldo correctos. Debe verificar que:

- Los datos sean leídos o escritos correctamente del disco duro cuando se realiza la copia de respaldo.
- No se hayan producido fallas en el medio de la copia de respaldo mientras se escribía en él.
- Los datos no se hayan malogrado mientras residían en el medio de la copia de respaldo.
- Los datos no sean restablecidos en sectores defectuosos del disco.
- Los datos sean correctamente escritos en el disco duro cuando se desea restablecerlos.

Algunas veces se utilizan programas de copias de respaldo que, a modo de verificación, leen o escriben los datos dos veces por seguridad, duplicando el tiempo que tarda una copia normal. Muchas veces es difícil recuperar los datos si se encuentran errores.

8.2.3 Alternativas de programas

Se debe elegir un programa de copia de respaldo adecuado, que tenga varias opciones y que sea fácil de usar. En el mercado se puede encontrar muchos utilitarios de copia de respaldo, dependiendo de las necesidades de los usuarios. Sin embargo, muchas veces, en

las unidades de cinta, la copia de respaldo sólo funciona con el programa que lo acompaña.

8.2.4 Características

La velocidad con que se realizan las copias de respaldo es demasiado lenta, particularmente si se hace con disquetes, puesto que tienen que ser cambiados en tiempos breves obligando a la persona a no desviar la atención de ellos.

Sin embargo, también se debe tener en cuenta la flexibilidad, fiabilidad y facilidad, y no guiarse porque un programa funciona más rápido que otro.

8.2.5 Facilidades de uso

Las sesiones de copia de respaldo son generalmente cortas, puesto que sólo se copia una pequeña parte del disco duro, aunque muchas veces pasa mucho tiempo en poner en movimiento el programa.

8.2.6 Rendimiento

La velocidad de la copia de respaldo, en cierto modo, la establece el equipo más que el programa. Las copias de respaldo se pueden acelerar optimizando el rendimiento del disco duro, teniendo disponibles grandes cantidades de memoria.

En los disquetes las copias de respaldo van deprisa, porque las unidades son más rápidas. En algunas unidades de cinta la copia de respaldo funciona más rápido que otras debido a la forma en que son formateados los datos.

8.3 Formas de realizar una copia de respaldo

Cuando los archivos se encuentran muy fragmentados y están esparcidos por los cilindros del disco, la copia de respaldo toma más tiempo puesto que para la lectura hay mayor movimiento de las cabezas. Para que la copia de respaldo sea rápida los archivos deben estar compactados en el mínimo número posible de cilindros. Las copias de respaldo pueden hacerse de dos formas:

8.3.1 Copia de respaldo de imagen

La copia de respaldo de imagen hace una copia exacta de la superficie del disco sin tener en cuenta la distribución de los archivos. Es rápido porque mueve una sola vez las cabezas de lectura y escritura a cada cilindro.

Las copias de respaldo de imagen son ideales para restablecer el disco entero después de un desastre importante o restablecer a un disco nuevo de las mismas características.

8.3.2 Copia de respaldo archivo a archivo

Con esta forma se graban archivos enteros uno a continuación de otro. Se puede restablecer cualquier archivo, o un grupo de ellos, sin alterar el resto de los datos del disco. Se puede usar para cambiar de discos de diferentes características y tamaños.

8.4 Tipos de copias de respaldo

Dependiendo de las necesidades de cada usuario se pueden hacer seis tipos de copias de respaldo y cada uno tiene su propia aplicación. Estos son:

8.4.1 Copias de respaldo globales

Se pueden copiar todos los datos del disco duro, incluyendo la estructura del árbol y los archivos del sistema.

8.4.2 Copias de respaldo parciales

Se puede copiar un grupo relacionado de archivos y crea una "imagen" de los datos en un determinado momento.

8.4.3 Copias de respaldo increméntales

Se puede copiar todos los archivos que han sido modificados desde la copia anterior.

8.4.4 Copias de respaldo simultáneas

Cuando los sistemas de imagen espejo pueden escribir datos dos veces en dos discos duros idénticos.

8.4.5 Copias de respaldo temporales

Son segundas copias de archivos que se guardan en el disco duro junto con los originales.

8.4.6 Copias de respaldo en serie

Se hace una serie de copias del mismo archivo, capturando cada etapa de su evolución.

8.7 Organización del ambiente para realizar una copia de respaldo

Las copias de respaldo realizadas en disco o en cinta, deben ser etiquetados y correctamente organizados para conocer en todo momento las últimas versiones y pueda localizarse fácilmente cuando se quiera restablecer los datos en el disco duro.

Para organizar el medio en que se va a realizar la copia de respaldo se pueden seguir los siguientes pasos:

8.7.1 Etiquetado

Cada disquete o cartucho debe ser etiquetado usando un código sencillo que indique a que lugar del sistema de copia pertenece y con un número de secuencia.

En los disquetes, la serie de etiquetas deberá tener un número secuencial que comience con el No. 1 y deben estar formateados y etiquetados antes de hacer la copia.

8.7.2 Mantener un registro

Todos los disquetes o cartuchos necesitan algún tipo de registro escrito del contenido que hay en él y la fecha de cuando ha sido grabado.

8.7.3 Almacenamiento

Los grupos de disquetes o cartuchos deben guardarse en sus propios contenedores, marcados cada uno con sus propias etiquetas y registros. Pueden ser almacenados en un ambiente externo al área de trabajo para prevenir la pérdida de los datos.

8.7.4 Rotación

Se debe instaurar procedimientos y un control de registro para ver que las copias de respaldo se han efectuado y que las copias cruciales se han enviado a un lugar seguro fuera de la instalación. La frecuencia de renovar la copia de respaldo que se tiene en otro lugar depende de la importancia de los datos.

8.8 Consideraciones al hacer una recuperación

Los programas que se utilizan para realizar una copia son en realidad programas de copia-recuperación. Con frecuencia se busca que las copias sean más rápidas y flexibles. Sin embargo, también se debe prestar atención a la recuperación de los datos cuando se produce algún percance.

A veces no es fácil recuperar los datos de la forma que se necesitan. Generalmente, sólo se desea recuperar un archivo, otras veces, recuperar los archivos que tienen una determinada extensión que cae dentro de dos fechas y en otros casos, restablecer un archivo en otro diferente al directorio del que han sido copiados.

Por lo mencionado debe tenerse en cuenta lo siguiente:

8.8.1 Puntos importantes

Es difícil restablecer una copia archivo a archivo de una copia de imagen. Una copia de imagen restablece los datos en el disco en el mismo orden que estaban anteriormente, a diferencia de los archivos fragmentados que están esparcidos por todo la copia. Ahora, las unidades de copia en cinta vienen con programas que puede hacer restablecimientos

archivo a archivo, partiendo de una copia de imagen, aunque el proceso lleva mucho tiempo.

8.8.2 Copia de respaldo de práctica

Se debe hacer copia de respaldo de práctica y estudiar todas las funciones de restauración para recuperar los datos cuando en realidad se necesiten, esto, con la finalidad de tener mayor confiabilidad en las copias.

8.8.3 Copias de respaldo atendidas frente a copias automáticas

Se puede realizar una copia a través de una tarjeta controladora especial, que mantiene automáticamente una copia idéntica (una imagen espejo) de un disco en un segundo disco idéntico, copiando en el segundo cada vez que se hace una operación de escritura.

Los discos flexibles pueden a veces servir para hacer copias automáticas, siempre y cuando sólo haya que meter y sacar unos pocos, cuando se graban los archivos.

Para hacer copias automáticas se puede requerir de equipo especial, pero también el programa es muy importante (excepto con los sistemas de imagen espejo).

El programa se encuentra en memoria, vigilando el reloj del sistema. Una copia puede hacerse cuando no se está utilizando la máquina o se puede hacer constantemente en background mientras el ordenador está siendo usado.

8.8.4 Copias de respaldo fuera de horas

La forma más frecuente es hacer las copias fuera de las horas de trabajo, pero esto puede requerir cierta atención. La copia sólo la puede iniciar el programa, por lo que tiene que estar activo cuando se vaya a efectuar la copia.

El programa puede estar en la memoria o cargarse al final de la jornada de trabajo. Se recomienda dejar la máquina encendida y que la hora del sistema tenga la hora correcta.

8.8.5 Copias de respaldo en Background

Funcionan como programas residentes en memoria, buscando los archivos que hayan sido modificados para hacer su tarea. Cuando comienzan las copias, éstos se realizan al mismo tiempo que cualquier otra tarea que se esté haciendo en la máquina.

8.8.6 Refrescamiento o regeneración

Cada cierto tiempo que se considere necesario, de acuerdo al tiempo medio de duración, se reemplazará las copias por un nuevo juego de medios de almacenamiento.

8.8.7 Prueba de las copias de respaldo

Una vez concluido la copia, se hará una restauración para comprobar que la copia se ha realizado con éxito.

8.9 Bodega de archivos magnéticos

8.9.1 Cajas fuertes de alta seguridad contra incendios para archivar medios de almacenamiento

Tanto el archivo interno de la organización, como el externo (ubicado fuera de la organización) donde se van a guardar los medios de almacenamiento que contienen la información que se quiere resguardar adecuadamente, deben contar con bóvedas, cuyos ambientes sean especialmente diseñados para su custodia. Dichos ambientes presentarán las siguientes características. El acceso a los ambientes donde se encuentran las cajas debe ser restringido

8.9.2 Puertas de acceso para la bóveda y contra incendios

El ambiente presentará todas las medidas de seguridad como son puerta de bóveda para su acceso, sistema contra incendios e inundaciones y sistemas de alarmas. Para combatir el fuego se tienen algunos de los siguientes elementos:

- Sistemas Automáticos Antifuego

- Sprinklers. Es un sistema "Tipo Ducha". La instalación de este sistema se efectúa en la parte superior del ambiente, como el techo.

- Inundación del área con gas. Otro de los métodos es la inundación del área con gas antifuego. En una emergencia por fuego, el área se inunda con un determinado gas como:

- Dióxido de Carbono, Halón.

- Extinguidores manuales Cuando no se cuenta con sistemas automáticos antifuego y se vea o perciba señales de fuego, entonces se debe actuar con rapidez para poder sofocar el incendio.

CAPÍTULO 9

9 Seguridad en Internet

9.1 Introducción

Es importante tener una política de seguridad de red efectiva y bien pensada que pueda proteger la inversión y recursos de información de la organización . Una política de seguridad de red justifica su uso, sólo si vale la pena proteger los recursos e información que tiene la organización en las redes. La mayoría de las organizaciones tienen información sensible y secretos importantes en sus redes. Esta información debería ser protegida contra el vandalismo del mismo modo que otros bienes valiosos.

La mayoría de los diseñadores de redes, por lo general, comienzan con la implementación de soluciones de barreras de protección antes de que ningún problema de seguridad de red haya sido identificado en forma acertada. Tal vez una razón para esto sea que establecer una política efectiva de seguridad de red signifique formular algunas preguntas difíciles con relación a qué tipos de servicios de trabajo y recursos de Internet va a permitir que tengan acceso los usuarios, y cuáles tendrá que restringir debido a los riesgos de seguridad.

Al diseñar la política de red que se debiera usar, es tal que no disminuirá la capacidad de la organización . Una política de red que evita que los usuarios cumplan con sus tareas en forma efectiva, puede tener consecuencias indeseables: los usuarios de la red podrán encontrar formas de ignorar su política de red, convirtiéndola en algo inútil.

Una política de seguridad de red efectiva es algo que todos los usuarios de la red y administradores pueden aceptar, y están dispuestos a reforzar.

9.2 Hacker

Es un término en la jerga informática que define a una persona que tiene conocimientos informáticos muy avanzados y que disfruta de explorar sistemas y programas de computadoras, algunas veces al punto de obsesión.

Este tipo de personas a menudo quiebra la seguridad en las redes de computadoras de las organizaciones privadas y/o gubernamentales. Estas personas suelen manejar varios lenguajes de programación. Trabajan muchas veces sobre los sistemas UNIX, conocen firmemente la implementación de TCP/IP así como protocolos de comunicación.

Una vez que un Hacker ha quebrado la seguridad de las redes de computadoras, iría en contra de la ética de los Hackers hacer alguna alteración a los datos a los cuales tienen acceso.

9.3 Cracker

La definición de Cracker es alguna persona que intenta quebrar un sistema, a través de la búsqueda automatizada o adivinando nombre de usuarios y/o contraseña que permitan accesar a los sistemas. Usualmente estas personas son jóvenes que son muy maliciosos y al estar dentro de algún sistema destruyen o dañan información en los sistemas.

9.4 Política de seguridad del sitio

Una organización puede tener muchos sitios y cada uno contar con sus propias redes. Sí la organización es grande, es muy probable que los sitios tengan diferentes administradores de red, con diferentes metas y objetivos. Si estos sitios no están conectados por medio de una red interna, cada uno de ellos podrá tener sus propias políticas de seguridad de red. Sin embargo, si los sitios están conectados por una red interna, la política de red deberá agrupar las metas de todos los sitios que estén interconectados.

En general, un sitio es cualquier parte de la organización que posee computadoras y recursos relacionados con la red. Dichos recursos incluyen, pero no se limitan a los siguientes:

- Estaciones de trabajo
- Computadoras anfitrión y servidores
- Dispositivos de Interconexión: routers, bridges
- Servidores de terminal
- Software para red y aplicaciones
- Cables de red
- Información en archivos y bases de datos

9.5 Firewall

Los Firewalls son un tipo de seguridad muy efectiva en redes. Intenta prevenir los ataques de usuarios externos a la red interna. Tiene múltiples propósitos:

- Restringir la entrada a usuarios a puntos cuidadosamente controlados.
- Prevenir los ataques
- Restringir los permisos de los usuarios a puntos cuidadosamente controlados.

Un Firewall es a menudo instalado en el punto donde la red interna se conecta con Internet. Todo tráfico externo de Internet hacia la red interna pasa a través del Firewall, así puede determinar si dicho tráfico es aceptable, de acuerdo a sus políticas de seguridad. Lógicamente un Firewall es un separador, un analizador, un limitador. La implementación física varia de acuerdo al lugar. A menudo, un Firewall es un conjunto de componentes de hardware - un router, un host, una combinación de routers, computadoras y redes con programas apropiados.

Rara vez es un simple objeto físico. Usualmente esta compuesto por múltiples partes y alguna de esas partes puede realizar otras tareas. La conexión de Internet también forma parte del Firewall.

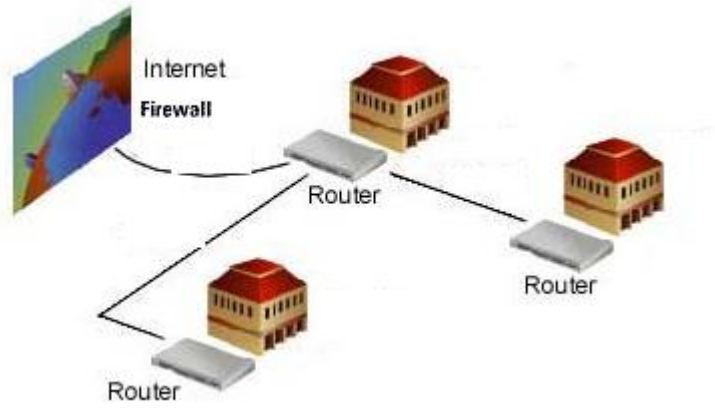


Figura 9.1
Fuente: http://www.cisco.com

Un Firewall es vulnerable, él no protege de la gente que está dentro de la red interna. El Firewall trabaja mejor si se complementa con una defensa interna.

Un Firewall es la forma más efectiva de conectar una red a Internet y proteger su red. Los Firewalls también tienen otros usos. Por ejemplo, se pueden usar para dividir partes de un sitio que tienen distintas necesidades de seguridad.

Las dos principales aproximaciones usadas para construir Firewalls hoy son:

- Filtrado de paquetes
- Servicio Proxy

9.5.1 Filtrado 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 filtrar paquetes en un Firewall es

conocido como "screening router".

9.5.2 Servicio Proxy

Este es un servicio altamente utilizado en Internet por muchos proveedores de acceso y organizaciones con conexión a la red. Lo que realiza el servidor Proxy es almacenar datos, cómo imágenes y páginas Web, para que cuando un usuario requiere información, ésta sea proporcionada desde el servidor Proxy. De esta manera, el tiempo de carga de la información es mucho menor, porque no se debe recibir la información desde Internet. Además, si la información no se encuentra en el Proxy, esta es buscada en Internet, pero ya quedará almacenada para que en futuras sesiones, la información provenga del Proxy, con lo que navegar se vuelve un proceso rápido.

Este servicio se debe configurar en un programa cliente como un browser (Internet Explorer, Netscape Navigator), ya que el Proxy actúa como un "filtro" entre su programa y la red Internet.

Una vez configurado el servicio del lado del cliente, toda conexión que usted intente realizar hacia Internet llegará primero al Proxy; si la información ya está allí almacenada, el mismo Proxy la entrega al usuario, de lo contrario, este contacta la fuente de los datos (en Internet), los pasa al cliente y los almacena para futuras consultas de otros usuarios.

9.6 Sniffers

Un sniffer es un pequeño dispositivo físico o "lógico" que permite "ver" la información que transita por la máquina o el servidor. No solamente captura los textos que contiene la máquina sino toda la información de las máquinas de donde provino la información.

Un sniffer puede servir para detectar las fallas de seguridad, pero también puede ser utilizado de manera indebida para interceptar los puntos de donde proviene la información.

GLOSARIO

AppleTalk
Es una red de área local (LAN) construida para las computadoras Apple Macintosh y las impresora Laser. Este soporta el esquema del cableado Apple's LocalTalk así como Ethetnet y Token Ring.

Ataque
Intento de transgredir los controles de seguridad de un sistema de información. El ataque puede alterar, borrar, modificar la base de datos. El ataque depende de la vulnerabilidad del sistema.

Auditoría
Examen independiente de los registros y actividades de acuerdo a los controles establecidos, procedimientos operacionales y operaciones legales, recomienda cambios ratifica los establecidos.

CD ROM
Abreviación de Compact Disc Read Only memory. Es un tipo de disco óptico capaz de almacenar hasta 650Mb de datos. Un CD tiene la capacidad de 700 disquetes. Actualmente la nueva tecnología de CD permite la escritura y re escritura.

Confidencialidad:
Asegura que la información se mantendrá secreta y con los límites apropiados a los usuarios.

CPU
Abreviación de "Central Processing Unit", que se puede definir como el cerebro de la computadora y es donde se registran los cálculos que son requeridos por algún programa.

Un CPU tiene 2 componentes: La unidad lógica y aritmética (ALU) y la unidad de control que extrae las instrucciones de la memoria y las ejecuta. Ambas trabajan para presentar el resultado.

Criptografía
La ciencia concerniente a los principios y métodos referente a convertir por medio del encriptado de un texto legible a un texto ilegible y luego volverlo a su forma original.
DES (Data Encryption Standard)

Es un cripto algoritmo desclasificado utilizado por The National Bureau of Standards para uso público para la protección de información descalificada y publicada por the Federal Processing Standard.

Ethernet
Protocolo de una de área local, desarrollado por Xerox Corporation en cooperación con DEC e INTEL en 1,976. Este protocolo utiliza una topología de bus o estrella y soporta velocidad para transferir datos de 10Mbps. Una nueva versión de Ethernet llamada 100Base-T o Fast Ethernet soporta hasta 100Mbps. Así como la más reciente versión que soporta hasta 1 gigabit por segundo.

Hacker
Persona que disfruta explorando los detalles de las computadoras y como extremas sus capacidades de una forma maliciosa o inquisitiva tratando de descubrir información y los detalles de programación del sistema. Es la persona opuesta a las que prefieren aprender lo mínimo necesario.

Hardware
Se refiere al equipo propiamente dicho, es decir los componentes que se pueden tocar, tal como un disco duro, el teclado el monitor, una tarjeta, etc.

Huellas de auditoría
En un sistema de computadora los registros cronológicos son recursos que se utilizan para ejecutar una auditoría. Estos incluyen archivos de accesos, sistema de contraseñas, bitácora del sistema y registra cualquier intento de violar la seguridad, registra los ingresos no autorizados y los autorizados.

Integridad
Aseguramiento que la información no será accidentalmente o maliciosamente alterada o destruida.

IPX
Siglas que significan “Internetwork Packet Exchange” y es un protocolo de red que es utilizado por el sistema operativo de Novell Netware

Novell Netware
Es el Sistema operativo de red de área local más popular a nivel mundial. Como otras compañías de software, Novell también esta respondiendo a la repentina popularidad de Internet e Intranet, se unió a Netscape para formar una nueva compañía llamada Novonyx, que integrará los productos de Netscape para intranet con los productos de Novell.

Novell fue fundada en 1983 y su casa matriz se encuentra ubicada en Utah U.S.A.

OS/2X
Es un sistema operativo desarrollado por MicroSoft Corporation e IBM para computadoras personales, pero es vendido y administrado por IBM. OS/2 es compatible con DOS y Windows lo que permite ejecutar programas de ambas plataformas, sin embargo programas desarrollados para OS/2 no pueden ser ejecutados en Windows y DOS.

PC
Siglas de las palabras en ingles "Personal Computer" . La primera computadora personal fue producida para IBM a la que le llamaron PC.

Protocolo
Métodos de comunicación utilizados por las computadoras. Son especificaciones que describen reglas y procedimientos del flujo de actividades a ejecutar.

Seguridad de la red
Protección de las redes de computadoras y sus servidores de modificaciones sin autorización, destrucción y aseguramiento que la red trabajara en situaciones criticas correctamente sin tener efectos no deseados. La seguridad de la red incluye la integridad de los datos.

Sniffer
Es un programa que captura datos a lo largo de la red. Usado por hachers para capturar identificaciones, nombres y contraseñas. Es una herramienta de software que audita e identifica el trafico de paquetes en la red. También es usado legítimamente en las operaciones de la red y por el personal de mantenimiento para resolver problemas concernientes a la red de computadoras.

Software
Se refiere a los programas y datos que permite inter actuar al usuario con la computadora.

SPX
Siglas que significan "Sequenced Packet Exchange" que es la capa de transporte en el protocolo (capa 4 en el modelo OSI), el que es utilizado por redes de Novell Netware y provee el servicio de conexión entre 2 nodos de la red. SPX es utilizado por aplicaciones cliente/servidor.

TCP/IP
Siglas que significan "Transmission Control Protocol/Internet Protocol", el cual es el protocolo utilizado en las comunciaciones para conectar los computadores anfitriones (host) en Internet.

Token Ring
Un tipo de red de computadoras las cuales están situadas esquemáticamente en un círculo. Un Token es un bit que viaja al rededor del círculo, el que permite comunicar y enviar paquetes a través de éste dentro de la red.

UNIX
Es un sistema operativo multi-usuario y multitareas, desarrollado por Bell Labs en la década 1970. Originalmente fue creado para uso de programadores. Las primeras versiones no fueron tan amigables pues el nombre de los comandos eran un tanto complejo, pero con las versiones gráficas, esto cambio totalmente.

UNIX fue el primer sistema operativo escrito en lenguaje de alto nivel, llamada leguaje C, lo que daba la facilidad de instarlos en cualquier computadora que tuviera un compilador C. Su portabilidad junto a su bajo precio, UNIX se convirtió rápidamente en el más popular sistema operativo en las décadas siguiente a su nacimiento.

Bell Labs distribuye UNIX con los programas fuentes, lo que significa que cualquier persona puede personalizar su SO.

Debido a su portabilidad, flexibilidad y poder, UNIX se convirtió en el líder de sistemas operativos para terminales de trabajo en una red. Históricamente ha sido menos popular en las computadoras personales (PC), pero ahora a emergido una nueva versión llamada Linux la cual está revitalizando a UNIX en todas las plataformas.

UPS
Abreviación de "uninterruptible power supply", que es un equipo que suple de corriente eléctrica a una computadora en el caso de un corte de energía eléctrica. La tecnología más avanzada de UPS permite la administración de UPS desde el computador.

Windows NT
Es la versión más avanzada del sistema operativo de Windows. NT que significa "Nueva tecnología" (New Technology) es un sistema operativo de 32bits con funciones multitareas.

Existen 2 versiones de Windows NT: Windows NT server que está diseñada para trabajar en los servidores de red y Windows NT Workstation para trabajar como sistema operativo en las computadoras personales.

BIBLIOGRAFIA

CYGANSKI,David / ORR, John — Information Technology Inside/Outside
Prentice Hall Hispanoamérica, S. A.
1999

H.A Technical Solution — High Availability Technology
Sitio en Internet:http://www.tech-sol.com

HEWLLET PACKARD — High Availability Technology
Sitio en Internet: http://www.hpvencp.com

INEI — Instituto Nacional de Estadística del Perú
Sitio en Internet:http://www.inei.gob.pe

JAMES A., Senn — Análisis y diseño de sistemas de Inf.
Prentice Hall Hispanoamérica, S. A.
1998

MOLLAR, Manuel — Jaume University
Sitio en Internet: http://moon.inf.uji.es/

WEBOPEDIA — Enciclopedia de términos de Informática
Sitio en Internet:
http://www.webopedia.com